Netopia® R2020 Dual Analog Router

FOR DATA COMMUNICATION

User's Reference Guide

netopia®

Copyright

Netopia, Inc.
2470 Mariner Square Loop
Alameda, CA 94501-1010
U.S.A.

Part Number

For additional copies of this electronic manual, order Netopia part number 6160022-PF-01

Printed copies

For printed copies of this manual, order Netopia part number TER2020/Doc
(P/N 6160022-00-01)

Contents

Welcome to the Netopia R2020 Dual Analog Router *User's Reference Guide*. This guide is designed to be your single source for information about your Netopia R2020 Dual Analog Router. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

This Table of Contents page you are viewing consists of hypertext links to the chapters and headings listed. If you are viewing this on-line, just click any link below to go to that heading.

Part I: Getting Started 7

Part II: Advanced Configuration 7

Part III: Appendixes 15

Configuration options for your Netopia R2020 Dual Analog Router

The Netopia R2020 can be used in different ways depending on your needs. In general, you will probably want to use it in one or more of the following ways: (Click on one of these links)

- “1. Small Office connection to the Internet” with several computers in your office sharing a single IP address (Network Address Translation enabled)
- “2. Small Office connection to the Internet” with a block of IP addresses (Network Address Translation disabled),
- “3. Direct Connection to a Corporate Office (Telecommuter)”
- “4. Configured to accept incoming dial-up connections”
- “5. Configured for two onboard and one external modem on the Auxiliary port”

This section is intended to give you a path to the appropriate installation and configuration instructions based on your intended use for the Netopia R2020.

1. Small Office connection to the Internet

For Small Office connections to the Internet, using a single dynamic IP address with Network Address Translation (NAT) enabled, you should use the following configuration option:

- the SmartStart™ Wizard, included on your Netopia R2020 CD.
  This is the fastest and simplest way to get you up and running with the minimum difficulty.

  For instructions on this option, see “Setting up your Router with the SmartStart Wizard” on page 3-3.

netopia®

2. Small Office connection to the Internet

For Small Office connections to the Internet, using a block of IP addresses (Network Address Translation disabled), you should use the following configuration tool:

- Easy Setup configuration using console-based management. This option allows maximum flexibility for experienced users and administrators.

  For instructions on this option, see "Console-based Management" on page 5-1 and "Easy Setup" on page 6-1.

3. Direct Connection to a Corporate Office (Telecommuter)

For direct connections to a Corporate Office, you can use either one of two configuration options:

- If you will be using Network Address Translation, use the SmartStart™ Wizard, included on your Netopia R2020 CD.

  For instructions on this option, see "Setting up your Router with the SmartStart Wizard" on page 3-3.

- If your corporate office assigns you a static IP address, use Easy Setup under console-based management. This option allows maximum flexibility for experienced users and administrators.

  For instructions on this option, see "Console-based Management" on page 5-1 and "Easy Setup" on page 6-1.

4. Configured to accept incoming dial-up connections

To configure the Netopia R2020 to accept incoming dial-up connections, you should use the following configuration method:

- To create one or more dial-in Connection Profiles for each dial-in user, see "Creating a new Connection Profile" on page 7-2.

  You do this using console-based management.

  For instructions on using console-based management, see "Console-based Management" on page 5-1

  For instructions on creating a Connection Profile to dial out to an ISP or corporate site, see "Easy Setup" on page 6-1.

5. Configured for two onboard and one external modem on the Auxiliary port

To configure the Netopia R2020 to use the two onboard modems and a third external modem on the Auxiliary serial port, you should use the following configuration options. This might be done to allow three separate simultaneous dial-in/dial-out connections or one or two aggregated dial-in/dial-out calls using Multilink PPP.

- Install the special optional modem cable available from your reseller or directly from Netopia.
- use the SmartStart™ Wizard, to configure your outbound connection to an ISP. For instructions on this option, see "Setting up your Router with the SmartStart Wizard" on page 3-3.
- manual configuration using console-based management. You simply attach your modem using the special modem cable, and enter the telephone number and modem init string in your WAN configuration. For instructions on this option, see "Adding an external modem" on page 4-4.

Part I: Getting Started

Chapter 1

Introduction

Overview

The Netopia R2020 Dual Analog Router is a full-featured, stand-alone, multiprotocol router for connecting diverse local area networks (LANs) to the Internet and other remote networks. The Netopia R2020 Dual Analog Router uses two 56Kbps V.90 modems communicating over standard analog telephone lines to provide your whole network with a high-speed connection to the outside world.

This section covers the following topics:

- “Features and capabilities” on page 1-1
- “How to use this guide” on page 1-2

Features and capabilities

The Netopia R2020 Dual Analog Router provides the following features:

- WAN connection over two analog phone lines using two built-in 56Kbps V.90 modems
- Support for a third (external) modem via the Auxiliary port
- Support for Multilink PPP to aggregate the separate analog modems into a single virtual data pipe of 112Kbps using the built-in modems or 168Kbps by adding an external 56Kbps modem
- Connectivity to Ethernet LANs via built-in 8 port 10Base-T hub with uplink switch
- Status lights (LEDs) for easy monitoring and troubleshooting
- SmartStart™ Wizard software for easy configuration over an Ethernet network connection. The SmartStart Wizard may include an optional automatic registration with one of several major ISPs, making the process as simple as completing a registration form. Using the alternate manual setting to configure the router for an ISP that’s not listed, the software allows you to configure your internal connection by entering just five fields: username, password, dialup number, DNS, and IP gateway.
- Built-in Basic Firewall and NetBIOS filtering
- Support for secure Virtual Private Networks (VPN). This feature allows seamless integration with the Microsoft Windows NT Server’s mobile user-to-LAN built-in VPN solution via Dial-up Networking, as well as suitability for LAN-to-LAN VPN applications using Netopia routers at both ends.
    - Point-to-Point Tunneling Protocol (PPTP) with Microsoft Point-to-Point Encryption (MPPE) for authentication and payload encryption for communicating with remote Windows NT servers.
    - RFC 2107 Ascend Tunneling Management Protocol (ATMP) with 56-bit DES for authentication and extensions to include payload encryption.
- SmartIP™ makes it simple and economical to connect a workgroup of users to the Internet or a remote IP network by using Network Address Translation and a single IP address. Multiple Network Address

Translation (MultiNAT) adds significant flexibility and security for a wide range of applications.

  - 1-to-1 static NAT mapping
  - Multiple Many-to-1 NAPT mappings on a single interface. NAPT addresses can be assigned to specific private address subnets
  - Mapped services (exports) can use multiple public addresses
  - Co-existent mapped and unmapped interfaces
  - NAT rules per interface, similar to filter rules

- Connection Metering offers system-wide time and packet-based connection metering and budgeting through web-based management screens. It allows monitoring and enforcing preset budget rules on three separate Connection Profiles. Internet browsers such as Netscape Navigator™ and Microsoft's Internet Explorer™ can be used.
- Support for IP and IPX routing for Internet and Intranet connectivity
- DHCP IP address serving (over Ethernet or a WAN link) which allows local or remote network nodes to automatically acquire an IP address dynamically from a designated pool of available addresses
- Support for Console-based management
- Support for remote configuration by your reseller, your network administrator, or technicians at Netopia, Inc.
- Wall-mountable, Bookshelf (Side-stackable), or Desktop-stackable design for efficient space usage
- AppleTalk support (available as a separate add-on AppleTalk kit, including a firmware feature set enhancement and custom HD-15 dual RJ-11 PhoneNET™ connector) allows for LocalTalk to Ethernet routing, assigning IP addresses to Macintosh users (MacIP), IP functionality for LocalTalk users, and AURP tunneling for connectivity between remote AppleTalk networks.
- Upgradeable to other WAN interfaces including ISDN and DSL. You can exchange one WAN module for a higher-speed module or an always-on connection and use the remaining V.90 modem for integrated backup.

How to use this guide

This guide is designed to be your single source for information about your Netopia R2020 Dual Analog Router. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

You can also print out all of the manual, or individual sections, if you prefer to work from hard copy rather than on-line documentation. The pages are formatted to print on standard 8 1/2 by 11 inch paper. We recommend that you print on 3-hole punched paper, so that you can put the pages in a binder for future reference. For your convenience, a printed copy is available from Netopia. Order part number TER2121/Doc.

This guide is organized into chapters describing the Netopia R2020's advanced features. You may want to read each chapter's introductory section to familiarize yourself with the various features available.

Use the guide's table of contents and index to locate informational topics.

Chapter 2

Making the Physical Connections

This section tells you how to make the physical connections to your Netopia R2020 Dual Analog Router. This section covers the following topics:

- "Find a location" on page 2-1
- "What you need" on page 2-1
- "Identify the connectors and attach the cables" on page 2-2
- "Netopia R2020 Dual Analog Router Status Lights" on page 2-6

Find a location

When choosing a location for the Netopia Router, consider:

- Available space and ease of installation
- Physical layout of the building and how to best use the physical space available in relation to connecting your Netopia Router to the LAN
- Available wiring and jacks
- Distance from the point of installation to the next device (length of cable or wall wiring)
- Ease of access to the front of the unit for configuration and monitoring
- Ease of access to the back of the unit for checking and changing cables
- Cable length and network size limitations when expanding networks

For small networks, install the Netopia R2020 near one of the LANs. For large networks, you can install the Netopia R2020 in a wiring closet or a central network administration site.

What you need

Locate all items that you need for the installation.

Included in your router package are:

- The Netopia R2020 Dual Analog Router
- A power adapter and cord with a mini-DIN8 connector
- An RJ-45 Ethernet cable
- Two standard RJ-11 telephone cables
- A dual DE-9 and mini-DIN8 to DE-9 console cable (for a PC or a Macintosh)
- The Netopia CD containing the SmartStart Wizard, an Internet browser, Adobe® Acrobat® Reader for

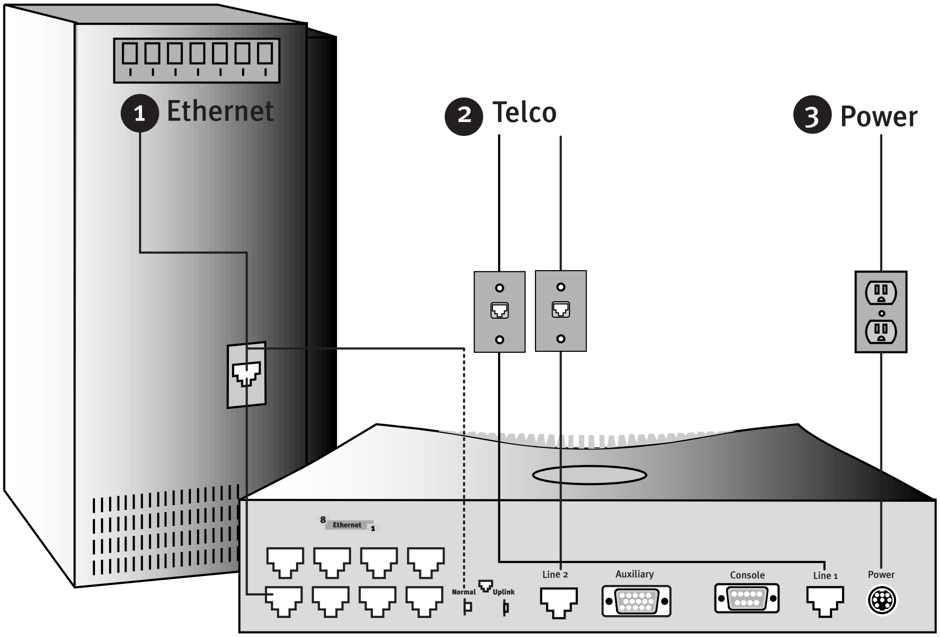
Windows and Macintosh, ZTerm terminal emulator software and NCSA Telnet 2.6 for Macintosh

You will need:

- A Windows 95-based PC or a Macintosh with Ethernet connectivity for configuring the Netopia R2020. This may be built-in Ethernet or an add-on card, with TCP/IP installed and configured. See "Before running SmartStart" on page 3-1.
- Two telephone lines, each with its own jack.

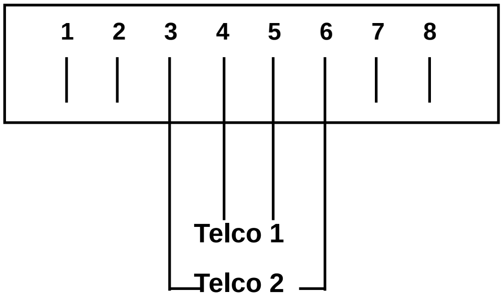
Identify the connectors and attach the cables

Identify the connectors and switches on the back panel and attach the necessary Netopia Router cables.



1. Connect the mini-DIN8 connector from the Power Adapter to the Power port, and plug the other end into an electrical outlet.
2. Connect one end of one of the RJ-11 cables to the "Line 1" port, and the other end to one of your wall outlets.

If you have two phone lines on a single wall outlet, this is the only Telco connection you need to make. The pinout configuration for the lines on the Line 1 port is shown in the following diagram:



Your first Telco number is carried on the inner pair and the second number on the outer pair.

3. If you have a second phone line with its own separate wall outlet, and want to use both built-in modems, connect one end of one of the RJ-11 cables to the "Line 2" port, and the other end to your second wall outlet.

4. Connect the Ethernet cable to any of the Ethernet ports on the router.

   (If you are connecting the router to an existing Ethernet hub, use Ethernet port #1 on the router and set the crossover switch to the **Uplink** position.)

   You should now have: the power adapter plugged in; the Ethernet cable connected between the router and your computer; and the telephone cables connected between the router and the wall outlets.

5. Insert your Netopia CD and follow the instructions to install an Internet browser and the Adobe Acrobat Reader, if you don't already have them.

6. Now, run the SmartStart application.

   SmartStart requires the following:

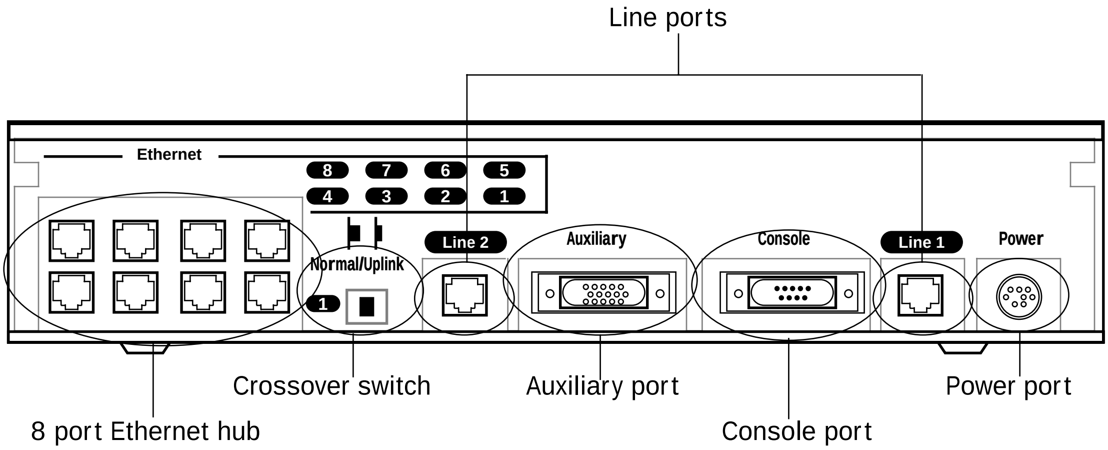
   - your computer must be Ethernet-capable, that is it must have both an Ethernet card and TCP/IP stack software. See "Before running SmartStart" on page 3-1.
   - your computer and the Netopia R2020 are powered ON.
   - the computer running SmartStart and the Netopia R2020 to be configured must be on the same Ethernet segment; there can be no intervening routers. Repeaters, such as 10Base-T hubs, are acceptable.

   Go to the section "Setting up your Router with the SmartStart Wizard" on page 3-3 for details on running SmartStart.

Netopia R2020 Dual Analog Router Back Panel Ports

The figure below displays the back of the Netopia R2020 Dual Analog Router.

Netopia R2020 Dual Analog Router back panel



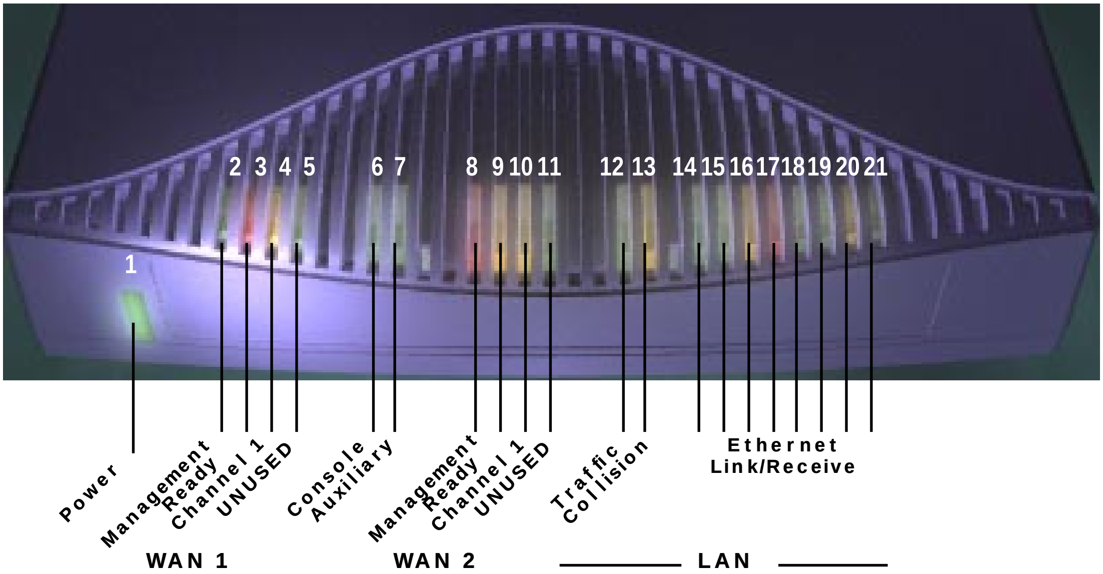
The following table describes all the Netopia R2020 Dual Analog Router back panel ports.

Port	Description
Power port	a mini-DIN8 power adapter cable connection.
Line 1 port	a **red** RJ-11 telephone jack labelled “Line 1".
Console port	a DE-9 Console port for a direct serial connection to the console screens. You may use this if you are an experienced user and choose not to use SmartStart. See “Connecting a local terminal console cable to your router” on page 5-3.
Auxiliary port	an HD-15 Auxiliary port for attaching an external modem or the optional AppleTalk kit.
Line 2 port	a **red** RJ-11 telephone jack labelled “Line 2". If you have only one telephone wall jack, supporting either one or two telephone numbers, use the “Line 1" port. “Line 1" supports two phone connections on a single line; “Line 2" supports a single phone connection.
Crossover switch	a crossover switch with Normal and Uplink positions. If Ethernet Port #1 is used for a direct Ethernet connection between a computer and the router, set the switch to the **Normal** position. If you are connecting the router to an Ethernet hub, use Ethernet port #1 on the router and set the switch to the **Uplink** position.
8-port Ethernet hub	Eight Ethernet jacks. You will use one of these to configure the Netopia R2020. For a new installation, you use the Ethernet connection. SmartStart only works over Ethernet. Later, if you want to do some advanced configuration, you can Telnet to the Console-based management screens via the Ethernet connection. You may also use the Console connection to run the Console-based management using a direct serial connection. You may either connect your computer directly to any of the Ethernet ports on the router, or connect both your computer and the router to an existing Ethernet hub on your LAN.

Netopia R2020 Dual Analog Router Status Lights

The figure below represents the Netopia R2020 status light (LED) panel.

Netopia R2020 LED front panel



The following table summarizes the meaning of the various LED states and colors:

When this happens...	the LEDs...
when the corresponding line is ringing	2 and 8 flash **yellow**
when the modem has carrier	3 and 9 are **green**.
when the router initiates an incoming or outgoing call	3 and 9 flash **green**
when data is transmitted or received	4 and 10 flash **yellow**.
when carrier is asserted	6 and 7 are **green**.
when console data is transmitted or received	6 and 7 flash **yellow**.
when data is transmitted or received by the ethernet controller	12 flashes **yellow**.
when the Ethernet interface detects a collision	13 flashes **red**.
when link is detected	14 though 21 are **solid green**.
when data is received on their respective ports	14 though 21 **flash green**

Chapter 3

Setting up your Router with the SmartStart Wizard

Once you've connected your router to your computer and your telecommunications line and installed a web browser, you're ready to run the Netopia SmartStart™ Wizard. The SmartStart Wizard will help you set up the router and share the connection. The SmartStart Wizard walks you through a series of questions and based on your responses automatically configures the router for connecting your LAN to the Internet or to your remote corporate network.

The SmartStart Wizard will:

- automatically check your Windows 95, 98, or NT PC's TCP/IP configuration to be sure you can accept a dynamically assigned IP address, and change it for you if it is not set for dynamic addressing
- check the physical connection from your computer to your router without your having to enter an IP address
- assign an IP address to your router
- allow you to register with a new ISP if you don't already have one. For a list of ISPs that support Netopia Routers in North America, see the Netopia website at http://www.netopia.com.
- allow you to enter your dial-up telephone numbers and other information, dial up and test your connection to your chosen ISP or other remote site

Before running SmartStart

Be sure you have connected the cables and power source as described in Step 1 "Connect the Router" guide contained in your Netopia folio.

Before you launch the SmartStart application, make sure your computer meets the following requirements:

	PC	Macintosh
System software	Windows 95, 98, or NT operating system	MacOS 7.5 or later
Connectivity software	TCP/IP must be installed and properly configured. See "Configuring TCP/IP on Windows 95, 98, or NT computers" on page 3-9	MacTCP or Open Transport TCP/IP must be installed and properly configured. See "Configuring TCP/IP on Macintosh computers" on page 3-13.
Connectivity hardware	Ethernet card (10Base-T)	Either a built-in or third-party Ethernet card (10Base-T)
Browser software	Netscape Communicator™ or Microsoft Internet Explorer, included on the Netopia CD. Required for web-based registration and web-based monitoring.	

<table>
<tr><th></th><th>PC</th><th>Macintosh</th></tr>
<tr><td colspan="3">Notes:
• The computer running SmartStart must be on the same Ethernet cable segment as the Netopia R2020. Repeaters, such as 10Base-T hubs between your computer and the Netopia R2020, are acceptable, but devices such as switches or other routers are not.
• SmartStart for the PC will set your TCP/IP control panel to “Obtain an IP address automatically” if it is not already set this way. This will cause your computer to reboot. If you have a specified IP address configured in the computer, you should make a note of it before running SmartStart, in case you do not want to use the dynamic addressing features built in to the Netopia Router and need to restore the fixed IP address.</td></tr>
</table>

Setting up your Router with the SmartStart Wizard

The SmartStart Wizard is tailored for your platform, but it works the same way on either a PC or a Macintosh. Insert the Netopia CD, and in the desktop navigation screen that appears, launch the SmartStart Wizard application.

SmartStart Wizard configuration screens

The screens described in this section are the default screens shipped on the Netopia CD. They derive from two initialization (.ini) files included in the same directory as the SmartStart application file. Your reseller or your ISP may have supplied you with customized versions of these files.

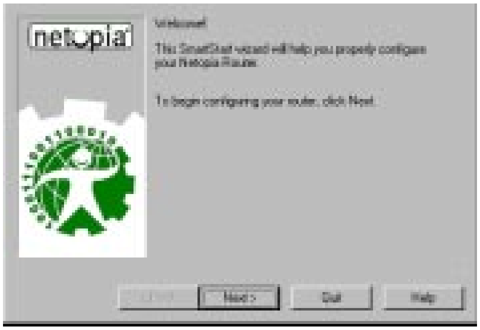
- If you have received a CD or diskette that has been customized by your reseller or ISP, you can run the SmartStart Wizard directly from the CD or diskette and follow the instructions your reseller or ISP provides. This makes your Netopia R2020 configuration even easier.
- If you have received only the .ini files from your reseller or ISP, perform the following:
  - Copy the entire directory folder containing the SmartStart Wizard application from the Netopia CD to your hard disk.
  - Copy the customized .ini files to the same directory folder that contains the SmartStart Wizard application, allowing the copy process to overwrite the original .ini files.
  - Run the SmartStart Wizard from your hard disk. You can then follow the instructions your reseller or ISP provides.

The SmartStart Wizard presents a series of screens to guide you through the preliminary configuration of a Netopia R2020. It will then create a connection profile using the information you supply to it.

Welcome screen. The first screen welcomes you to the SmartStart Wizard configuration utility.

Click the Next button after you have responded to the interactive prompts in each screen.

The Help button will display useful information to assist you in responding to the interactive prompts.



Welcome!

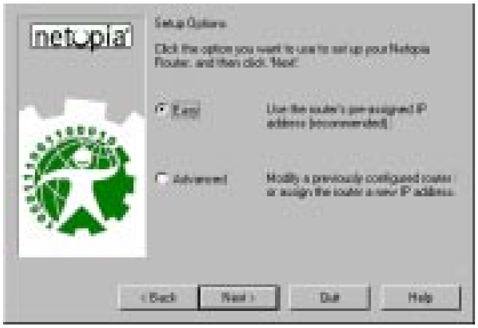
This SmartStart wizard will help you properly configure your Netopia Router.

To begin configuring your router, click Next.

Easy or Advanced options screen. You can choose either Easy or Advanced setup.

- If you choose Easy, SmartStart automatically uses the preconfigured IP addressing setup built into your router. This is the best choice if you are creating a new network or don’t already have an IP addressing scheme on your new network.

  If you choose Easy, you will see a “Connection Test screen,” like the one shown below while SmartStart checks the connection to your router.
- If you choose Advanced, skip to page 3-8 now. The SmartStart Wizard displays the “Router IP Address screen” on page 3-8, in which you can choose ways to modify your router’s IP address.



Setup Options

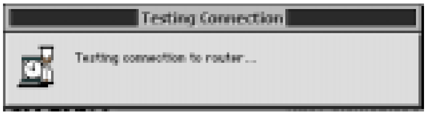
Click the option you want to use to set up your Netopia Router, and then click 'Next'.

● Easy — Use the router's pre-assigned IP address (recommended)

○ Advanced — Modify a previously configured router or assign the router a new IP address.

Easy option

Connection Test screen. SmartStart tests the connection to the router. While it is testing the connection, a progress indicator screen is displayed and the router’s Ethernet LEDs flash.



Testing Connection

Testing connection to router...

When the test succeeds, SmartStart indicates success.

If the test fails, the wizard displays an error screen. If the test fails, check the following:

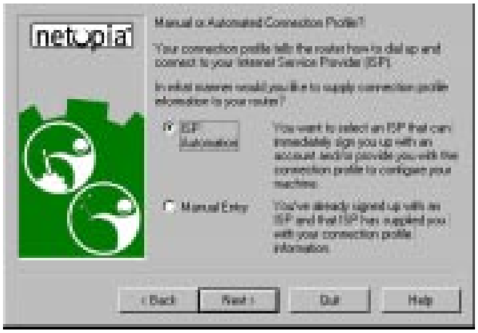
- Check your cable connections. Be sure you have connected the router and the computer properly, using the correct cables. Refer to the Step 1 “Connect the Router” sheet in your Netopia R2020 documentation folio.
- Make sure the router is turned on and that there is an Ethernet connection between your computer and the router.
- Check the TCP/IP control panel settings to be sure that automatic IP Addressing (Windows) or DHCP (Macintosh) is selected. If you are using a Windows PC, SmartStart will automatically detect a static IP address and offer to configure the computer for automatic addressing. On a Macintosh computer, you must manually set the TCP/IP Control Panel to DHCP. See “Configuring TCP/IP on Macintosh computers” on page 3-13. If you currently use a static IP address outside the 192.168.1.x network, and want to continue using it, use the Advanced option to assign the router an IP address in your target IP range. See “Advanced option” on page 3-8.
- If all of the above steps fail to resolve the problem, reset the router to its factory default settings and rerun SmartStart.

When the test is successful, you will see the "Manual or Automated Connection Profile screen," shown below.

Manual or Automated Connection Profile screen. The SmartStart Wizard asks you to select a method of creating a connection profile. The connection profile tells your router how to communicate with your ISP or other remote site, such as your corporate office. You can select either ISP Automation or Manual Entry.

Options are explained below.

Make your selection and click Next.



Manual or Automated Connection Profile?

Your connection profile tells the router how to dial up and connect to your Internet Service Provider (ISP).

In what manner would you like to supply connection profile information to your router?

● ISP Automation — You want to select an ISP that can immediately sign you up with an account and/or provide you with the connection profile to configure your machine.

○ Manual Entry — You've already signed up with an ISP and that ISP has supplied you with your connection profile information.

If you select ISP Automation, SmartStart offers you the option of choosing one of several Netopia ISP partners that support the Netopia R2020. You then see the "Internet Service Provider Selection screen" on page 3-5.

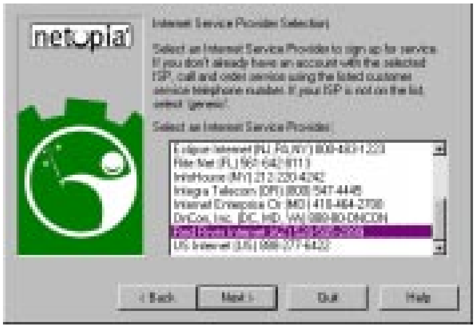
If you select Manual Entry, you must be prepared with the following information. You must enter:

- Your dial-up number, sometimes referred to as an ISP POP number
- Your Login name and Password. (These are case-sensitive.)
- Any PBX or Centrex phone system dialing prefix (such as "9" for an outside line)
- Your PPP authentication method. Options are: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), or None. Most ISPs use PAP; this is the default.
- Your Domain Name Server (DNS); this entry must be an IP address in dotted decimal format. (for example, 192.168.4.10, not "joe.isp.com")
- Optionally, an alternate DNS if your ISP provided one

If you select Manual Entry, the "Connection Profile screen," shown "Connection Profile screen" on page 3-6 appears.

Internet Service Provider Selection screen. Select an ISP from the list of Netopia ISP partners who have provided information for automatic setup. Choose Generic ISP if your ISP is not included on the list. If you don't already have an account with the selected ISP, call and order service using the listed customer service telephone number.

When you have done this, click Next.



Internet Service Provider Selection

Select an Internet Service Provider to sign up for service. If you don't already have an account with the selected ISP, call and order service using the listed customer service telephone number. If your ISP is not on the list, select 'generic'.

Select an Internet Service Provider:

Eclipse Internet [NJ, PA, NY] | 800-483-1223
Fiber Net [FL] | 561-642-8111
InfoHouse [NY] | 212-220-4242
Integra Telecom [OR] | (800) 547-4445
Internet Enterprise Ctr [MD] | 410-464-2700
DirCon, Inc. [DC, MD, VA] | 888-80-DNCON
[illegible]
US Internet [US] | 888-277-6422

- Most ISPs will provide you with information for you to enter in the "Connection Profile screen" on page 3-6 over the phone using the toll-free phone number shown in the scrolling list. Generally, they will provide you with:

- Your dial-up number, sometimes referred to as an ISP POP number
- Your Login name and Password. (These are case-sensitive.)

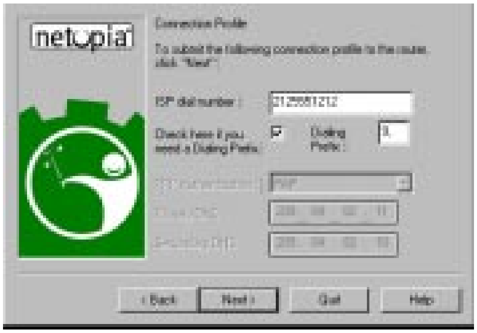
Note: Your ISP may provide you with additional values such as “Remote IP Gateway” or “Subnet Mask.” These entries are not required for the SmartStart Wizard to configure your router.

If you have a PBX or Centrex phone system, you may need a dialing prefix (such as “9” for an outside line). You will enter that information in the “Connection Profile screen,” shown below.

Connection Profile screen. Enter your ISP-supplied configuration information mentioned above. All fields must be filled in except the Alternate DNS field if your ISP does not provide one. If your ISP appeared in the “Internet Service Provider Selection screen” on page 3-5 your ISP will already have provided much of the information required for the connection, and these fields will appear grayed-out.

When you have done this, click Next.

The “Name and Password screen” on page 3-6 appears; this is where you enter the username and password for your connection to your ISP.



Connection Profile

To submit the following connection profile to the router, click "Next".

ISP dial number: 2125551212

Check here if you need a Dialing Prefix: ☑ Dialing Prefix: 9

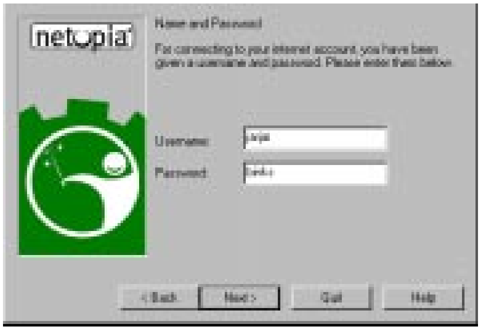
Name and Password screen. Enter the username and password that identifies you to your ISP. Your name and password can be up to 32 characters each.

Note: Some automated profiles already specify name and password for you. in this case, the screen is filled out for you and automatically skipped.

When you have done this, click Next.

The SmartStart Wizard then posts your connection profile information to your router.

Now the “Connection Profile Test screen,” (shown below) appears. It allows you to test your connection to your ISP using the connection profile you have just created.



Name and Password

For connecting to your internet account you have been given a username and password. Please enter them below.

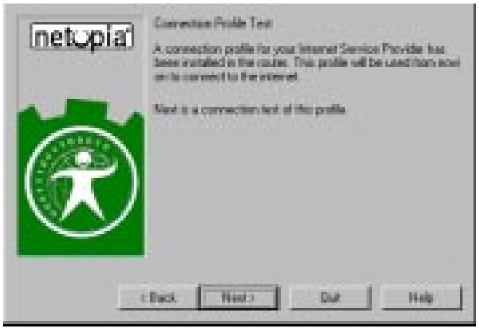
Username: [illegible]

Password: [illegible]

Connection Profile Test screen. SmartStart tests your connection profile by attempting to connect to your ISP.

To test the connection profile with your ISP, click Next.

While the test is running, SmartStart reports its progress in a brief succession of dialog boxes as described below.



Connection Profile Test

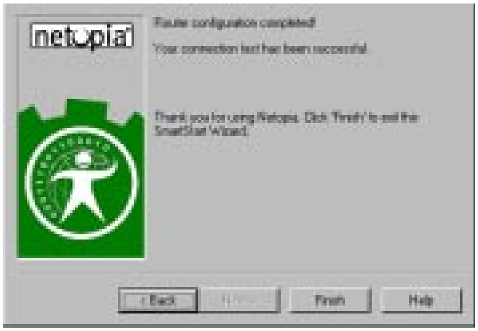
A connection profile for your Internet Service Provider has been installed in the router. This profile will be used from now on to connect to the Internet.

Next is a connection test of this profile.

Available Line Test Progress screen. SmartStart tests to see if the router can place calls on your telephone line. While it is testing the connection, a dialog box is displayed and the LEDs flash.

Connection Test Progress screen. SmartStart displays a dialog box showing you that your connection profile is being tested. If this test fails, check the physical connections between the computer, the router, and the wall jack or jacks. Check for errors in any manual entries you made during the configuration process.

Final screen. When the connection tests successfully, SmartStart displays a screen telling you that your configuration is now complete.



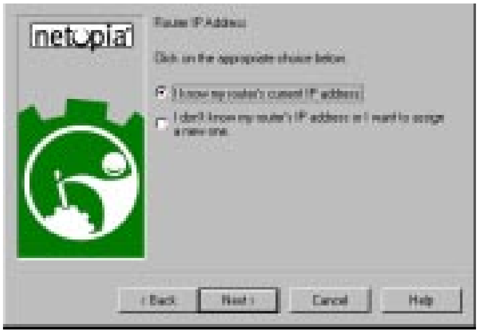
Router configuration completed!

Your connection test has been successful.

Thank you for using Netopia. Click 'Finish' to exit the SmartStart Wizard.

In most cases, this SmartStart configuration is all that you need to get your router up and running and connected to the Internet. However, you may want to take advantage of additional features or special configuration options available through the console-based configuration interface. For detailed instructions, see "Console-based Management" on page 5-1.

Advanced option



Router IP Address

Click on the appropriate choice below.

● I know my router's current IP address

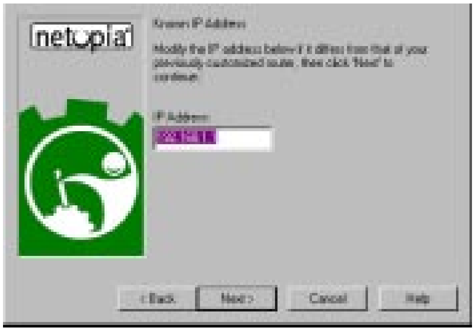
○ I don't know my router's IP address or I want to assign a new one.

Router IP Address screen. If you selected the Advanced option in the "Easy or Advanced options screen" on page 3-4, SmartStart asks you to choose between entering the router's current IP address and assigning an IP address to the router.

If the router has already been assigned an IP address, select the first radio button. If you do this, the "Known IP Address screen," appears (shown below.)

If you want to reconfigure the router with a new IP address and subnet mask, select the second radio button. If you do this, the "New IP Address screen" on page 3-8 appears.

When you have done this, click Next.



Known IP Address

Modify the IP address below if it differs from that of your previously customized router, then click "Next" to continue.

IP Address: [illegible]

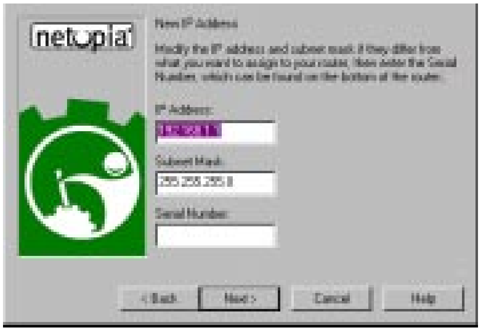
Known IP Address screen. SmartStart displays a recommended address for the router based on the IP address of the computer.

If you know the router has an IP address different from the default value, enter it now. Otherwise, accept the recommended address.

When you have done this, click Next.

SmartStart tests the connection to your router.

SmartStart then returns you to an "Connection Profile screen" on page 3-6.



New IP Address

Modify the IP address and subnet mask if they differ from what you want to assign to your router, then enter the Serial Number, which can be found on the bottom of the router.

IP Address: [illegible]

Subnet Mask: 255.255.255.0

Serial Number:

New IP Address screen. If you want to change the router's IP address, you enter the new IP address, the subnet mask, and the router's serial number in this screen. Remember, the serial number is on the bottom of the router. It is also found in your documentation folio.

Note: Forcing a new IP address may turn off the Netopia R2020's IP address serving capabilities, if you assign an IP address and subnet mask outside the router's current IP address serving pool. The Netopia R2020 does not allow an invalid address to be served. Use this option with caution.

When you have done this, click Next.

SmartStart forces the new IP address into the router, tests the connection, and then resets the router.

SmartStart then returns you to the "Manual or Automated Connection Profile screen" on page 3-5.

Sharing the Connection

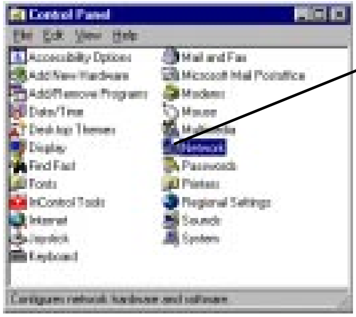
Configuring TCP/IP on Windows 95, 98, or NT computers

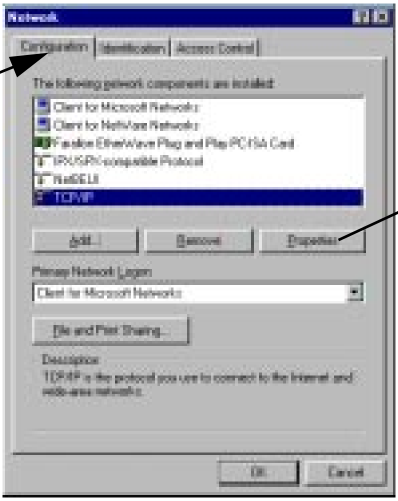
Configuring TCP/IP on a Windows computer requires the following:

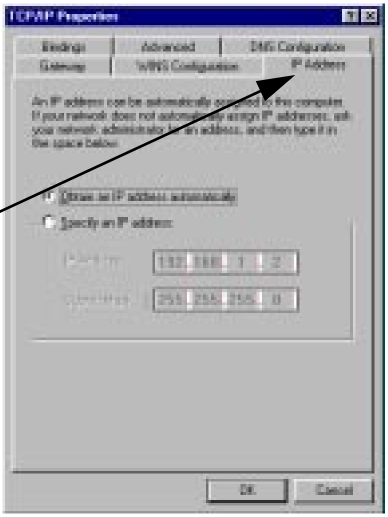
- An Ethernet card (also known as a network adapter)
- The TCP/IP protocol must be “bound” to the adapter or card

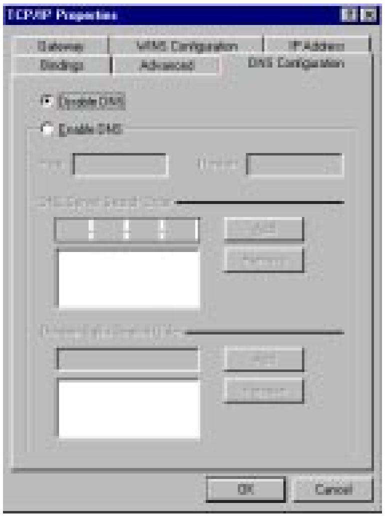
Dynamic configuration (recommended)

If you configure your Netopia R2020 using SmartStart, you can accept the dynamic IP address assigned by your router. The Dynamic Host Configuration Protocol (DHCP) server, which enables dynamic addressing, is enabled by default in the router. If your PC is not set for dynamic addressing, SmartStart will offer to do this for you when you launch it. In that case, you will have to restart your PC and relaunch SmartStart. If you configure your PC for dynamic addressing in advance, SmartStart need only be launched once. To configure your PC for dynamic addressing do the following:




Network
Configuration
Identification
Access Control
The following network components are installed:
Client for Microsoft Networks
Client for NetWare Networks
Farallon EtherWave Plug and Play PC/ISA Card
IPX/SPX-compatible Protocol
NetBEUI
TCP/IP
Add...
Remove
Properties
Primary Network Logon:
Client for Microsoft Networks
File and Print Sharing...
Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.
OK
Cancel


TCP/IP Properties
Bindings
Advanced
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
● Obtain an IP address automatically
○ Specify an IP address:
IP Address:
132 . 168 . 1 . 2
Subnet Mask:
255 . 255 . 255 . 0
OK
Cancel



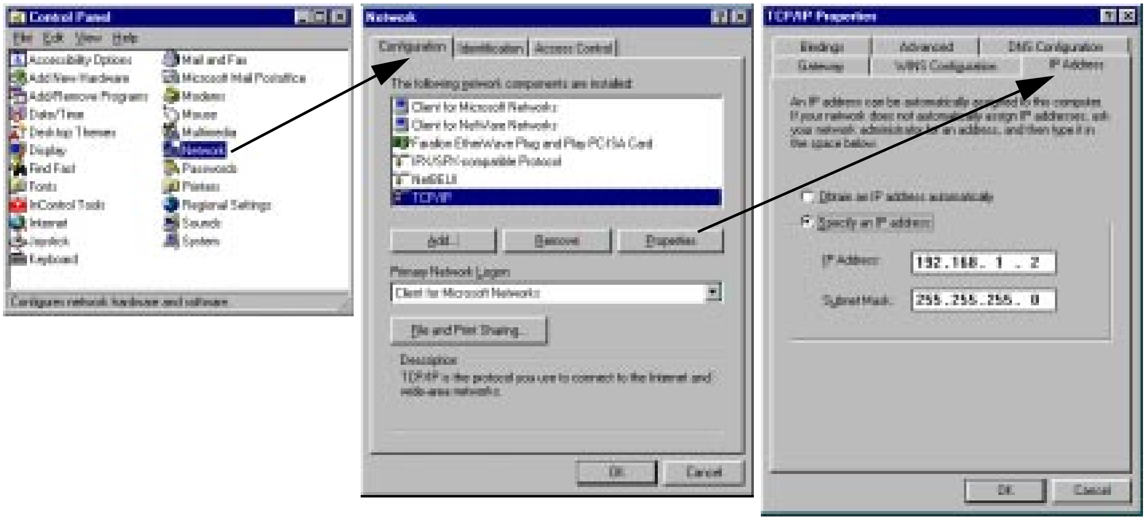
1. Go to the Start Menu/Settings/Control Panels and double click the Network icon. From the Network components list, select the Configuration tab.
2. Select TCP/IP-->Your Network Card. Then select Properties. In the TCP/IP Properties screen (shown below), select the IP Address tab. Click "Obtain an IP Address automatically."
3. Click on the DNS Configuration tab. Click Disable DNS. DNS will be assigned by the router with DHCP.
4. Click OK in this window, and the next window. When prompted, reboot the computer.

Note: You can also use these instructions to configure other computers on your network to accept IP addresses served by the Netopia R2020.

Static configuration (optional)

If you are manually configuring for a fixed or static IP address, perform the following:

1. Go to Start Menu/Settings/Control Panels and double click the Network icon. From the Network components list, select the Configuration tab.
2. Select TCP/IP-->Your Network Card. Then select Properties. In the TCP/IP Properties screen (shown below), select the IP Address tab. Click "Specify an IP Address."
   Enter the following:
   IP Address: 192.168.1.2
   Subnet Mask: 255.255.255.0
   This address is an example of one that can be used to configure the router with the Easy option in the SmartStart Wizard. Your ISP or network administrator may ask you to use a different IP address and subnet mask.



The following network components are installed:

- Client for Microsoft Networks
- Client for NetWare Networks
- Farallon EtherWave Plug and Play PC ISA Card
- IPX/SPX-compatible Protocol
- NetBEUI
- TCP/IP

Primary Network Logon: Client for Microsoft Networks

File and Print Sharing...

Description: TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

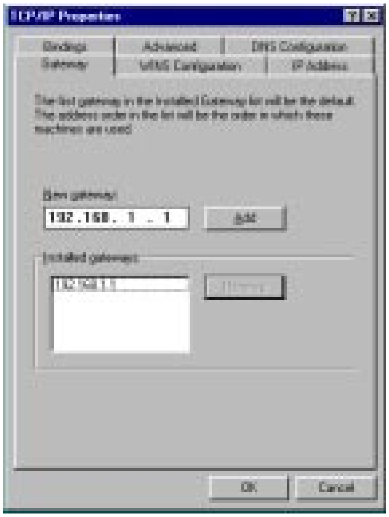
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

◉ Specify an IP address:

IP Address: 192.168. 1 . 2

Subnet Mask: 255.255.255. 0

3. Click on the Gateway tab (shown below). Under “New gateway,” enter 192.168.1.1. Click Add. This is the Netopia R2020’s pre-assigned IP address.

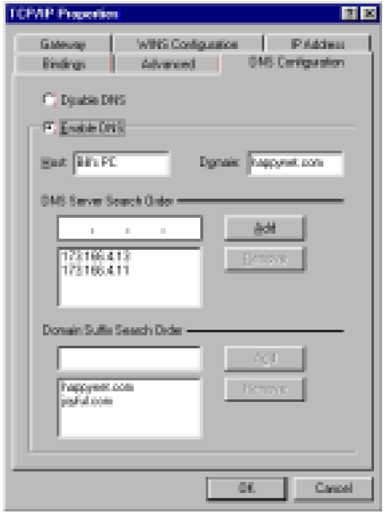


The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: 192.168. 1 . 1

Installed gateways: 192.168.1.1

Click on the DNS Configuration tab. Click Enable DNS. Enter the following information:



◉ Enable DNS

Host: Bill's PC

Domain: happynet.com

DNS Server Search Order: 173.166.4.13, 173.166.4.11

Domain Suffix Search Order: happynet.com, pghd.com

Host: Type the name you want to give to this computer.

Domain: Type your domain name. If you don't have a domain name, type your ISP's domain name; for example, netopia.com.

DNS Server Search Order: Type the primary DNS IP address given to you by your ISP. Click Add. Repeat this process for the secondary DNS.

Domain Suffix Search Order: Enter the same domain name you entered above.

4. Click OK in this window, and the next window. When prompted, reboot the computer.

Note: You can also use these instructions to configure other computers on your network with manual or static IP addresses. Be sure each computer on your network has its own IP address.

Configuring TCP/IP on Macintosh computers

The following is a quick guide to configuring TCP/IP for MacOS computers. Configuring TCP/IP in a Macintosh computer requires the following:

- You must have either Open Transport or Classic Networking (MacTCP) installed.

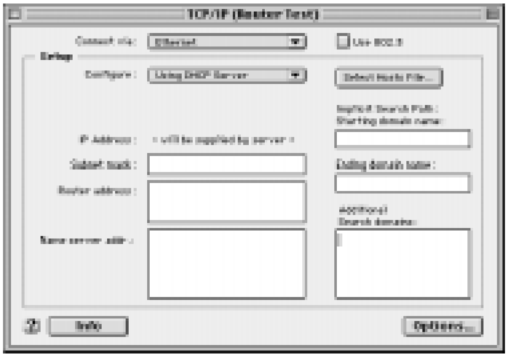
  Note: If you want to use the Dynamic Host Configuration Protocol (DHCP) server built into your Netopia R2020 to assign IP addresses to your Macintoshes, you must be running Open Transport, standard in MacOS 8, and optional in earlier system versions. You can have your Netopia R2020 dynamically assign IP addresses using MacTCP; however, to do so requires that the optional AppleTalk kit be installed which can only be done after the router is configured.

- You must have built-in Ethernet or a third-party Ethernet card and its associated drivers installed in your Macintosh.

Dynamic configuration (recommended)

If you configure your Netopia R2020 using SmartStart, you can accept the dynamic IP address assigned by your router. The Dynamic Host Configuration Protocol (DHCP), which enables dynamic addressing, is enabled by default in the router. To configure your Macintosh computer for dynamic addressing do the following:

1. Go to the Apple menu. Select Control Panels and then TCP/IP.
2. With the TCP/IP window open, go to the Edit menu and select User Mode. Choose Basic and click OK.
3. In the TCP/IP window, select “Connect via: Ethernet” and “Configure: Using DHCP Server.”



TCP/IP (Router Test)

Connect via: Ethernet

Configure: Using DHCP Server

IP Address: < will be supplied by server >

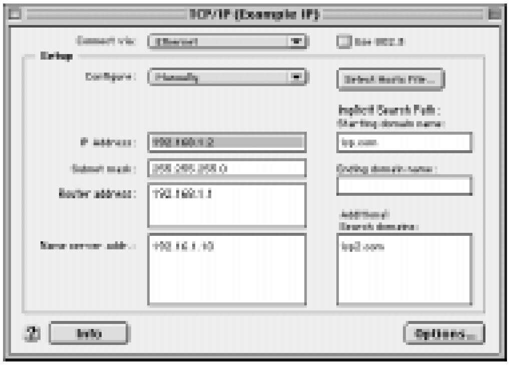
Note: You can also use these instructions to configure other computers on your network to accept IP addresses served by the Netopia R2020.

Static configuration (optional)

If you are manually configuring for a fixed or static IP address, perform the following:

1. Go to the Apple menu. Select Control Panels and then TCP/IP or MacTCP.
2. With the TCP/IP window open, go to the Edit menu and select User Mode. Choose Advanced and click OK.

   Or, in the MacTCP window, select Ethernet and click the More button.



TCP/IP (Example IP)

Connect via: Ethernet

☐ Use 802.3

Setup

Configure: Manually

IP Address: 192.168.1.2

Subnet mask: 255.255.255.0

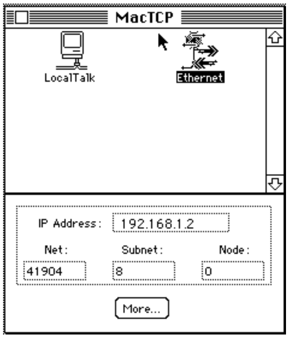
Router address: 192.168.1.1

Name server addr.: 192.16.1.10

Implicit Search Path: Starting domain name: isp.com

Ending domain name:

Additional Search domains: isp2.com



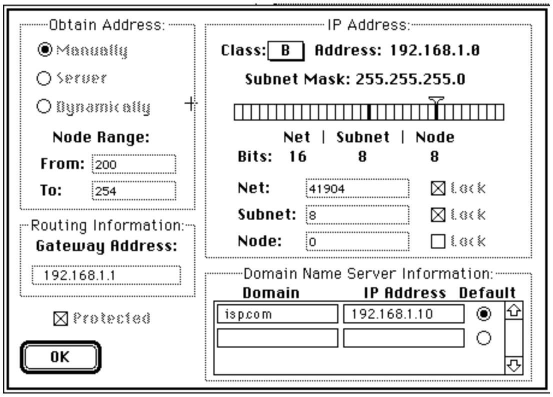
MacTCP

IP Address: 192.168.1.2

Net: 41904

Subnet: 8

Node: 0



Obtain Address:

● Manually

○ Server

○ Dynamically

Node Range:

From: 200

To: 254

Routing Information:

Gateway Address: 192.168.1.1

☒ Protected

IP Address:

Class: B Address: 192.168.1.0

Subnet Mask: 255.255.255.0

	Net	Subnet	Node
Bits:	16	8	8

Net: 41904 ☒ Lock

Subnet: 8 ☒ Lock

Node: 0 ☐ Lock

Domain Name Server Information:

Domain	IP Address	Default
isp.com	192.168.1.10	●
		○

3. In the TCP/IP window or in the MacTCP/More window, select or type information into the fields as shown in the following table.

Option:	Select/Type:
Connect via:	Ethernet
Configure:	Manually
IP Address:	192.168.1.2
Subnet mask:	255.255.255.0
Router address:	192.168.1.1
Name server address:	Enter the primary and secondary name server addresses given to you by your ISP
Implicit Search Path: Starting domain name:	Enter your domain name; if you do not have a domain name, enter the domain name of your ISP

4. Close the TCP/IP or MacTCP control panel and save the settings.
5. If you are using MacTCP, you must restart the computer. If you are using Open Transport, you do not need to restart. These are the only fields you need to modify in this screen.

Note: You can also use these instructions to configure other computers on your network with manual or static IP addresses. Be sure each computer on your network has its own IP address.

Dynamic configuration using MacIP (optional)

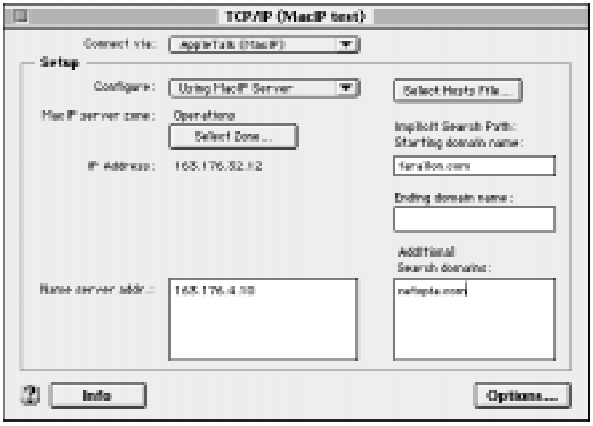
If you want to use MacIP to dynamically assign IP addresses to the Macintosh computers on your network you must install the optional AppleTalk feature set kit.

Note: You cannot use MacIP dynamic configuration to configure your Netopia R2020 Dual Analog Router because you must first configure the router in order to enable AppleTalk.

Once the AppleTalk kit is installed, you can configure your Macintoshes for MacIP. To configure dynamically using MacIP, perform the following:

Using Open Transport TCP / IP

1. Go to the Apple menu. Select **Control Panels** and then **TCP / IP**.
2. With the TCP / IP window open, go to the Edit menu and select **User Mode**. Choose **Advanced** and click **OK**.



TCP/IP (MacIP test)

Connect via: AppleTalk (MacIP)

Setup

Configure: Using MacIP Server

MacIP server zone: Operations

IP Address: 163.176.32.12

Implicit Search Path: Starting domain name: farallon.com

Ending domain name:

Additional Search domains: netopia.com

Name server addr.: 163.176.4.10

3. In the TCP / IP window, select or type information into the fields as shown in the following table.

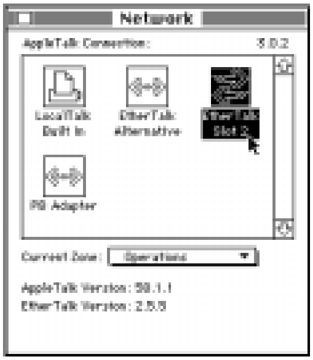
TCP / IP Option:	Select / Type:
Connect via:	AppleTalk (MacIP)
Configure:	Using MacIP server
MacIP Server zone:	(select available zone)
Name server address:	Enter the primary and secondary name server addresses given to you by your ISP
Implicit Search Path: Starting domain name:	Enter your domain name; if you do not have a domain name, enter the domain name of your ISP

4. Close the TCP / IP control panel and save the settings.

   These are the only fields you need to modify in these screens.

Using Classic Networking (MacTCP)

1. Go to the Apple Menu. Select **Control Panels** and then **Network**.
2. In the Network window, select **EtherTalk**.

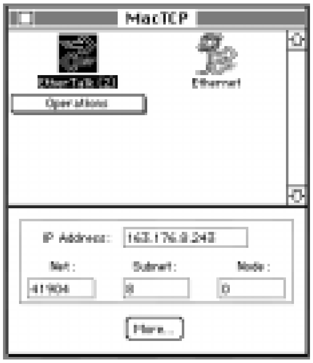


Network

AppleTalk Connection: 3.0.2

Current Zone: Operations

AppleTalk Version: 58.1.1
EtherTalk Version: 2.5.5

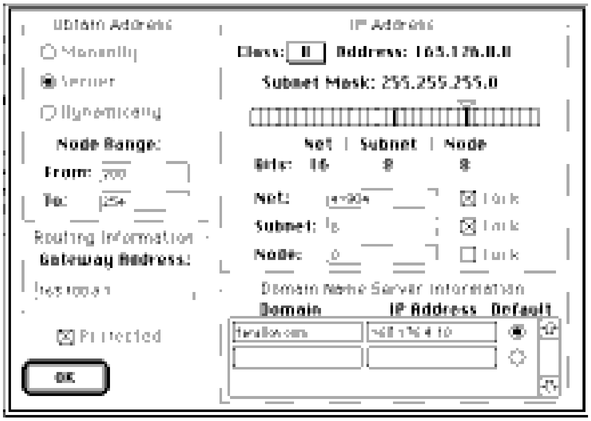


MacTCP

Operations

IP Address: 163.176.8.243

Net: 41904 Subnet: 8 Node: 0



Obtain Address
○ Manually
● Server
○ Dynamically

Node Range:
From: 200
To: 254

Routing Information
Gateway Address:
163.176.8.1

☒ Protected

IP Address
Class: B Address: 163.176.0.0
Subnet Mask: 255.255.255.0

	Net	Subnet	Node
Bits:	16	8	8

Net: 41904 ☒ Lock
Subnet: 8 ☒ Lock
Node: 0 □ Lock

Domain Name Server Information

Domain	IP Address	Default
farallon.com	163.176.4.10	●
		○

3. Go back to the Apple menu. Select **Control Panels** and then **MacTCP**.
4. Select **EtherTalk**.

   From the pull-down menu under EtherTalk, select an available zone; then click the **More** button.

   In the MacTCP/More window select the **Server** radio button. If necessary, fill in the Domain Name Server Information given to you by your administrator.
5. Restart the computer.

   These are the only fields you need to modify in these screens.

Note: More information about configuring your Macintosh computer for TCP/IP connectivity through a Netopia R2020 can be found in Technote NIR_026, "Open Transport and Netopia Routers," located on the Netopia Web site.

Chapter 4

Connecting Your Local Area Network

This chapter describes how physically to connect the Netopia R2020 to your local area network (LAN). Before you proceed, make sure the Netopia R2020 is properly configured. You can customize the Router's configuration for your particular LAN requirements using Console-based Management (see "Console-based Management" on page 5-1).

This section covers the following topics:

- "Overview" on page 4-1
- "Readying computers on your local network" on page 4-1
- "Connecting to an Ethernet network" on page 4-3
- "Adding an external modem" on page 4-4
- "Connecting to a LocalTalk network" on page 4-5

Overview

You can connect the Netopia R2020 to an IP or IPX network that uses Ethernet.

If you have purchased the AppleTalk feature expansion kit, you can also connect the Router to a LocalTalk network that uses PhoneNET cabling.

Additionally, you can connect a third (external) modem. See "Adding an external modem," below.

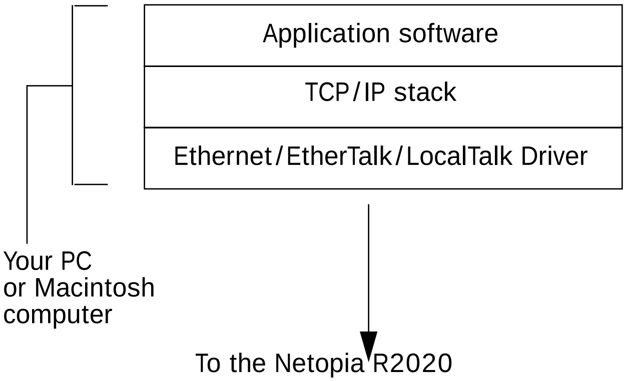
Caution!

Before connecting the Netopia R2020 to any AppleTalk LANs that contain other AppleTalk routers, you should read "Routers and seeding" on page 12-3.

See the sections later in this chapter for details on how to connect the Netopia R2020 to different types of networks.

Readying computers on your local network

PC and Macintosh computers must have certain components installed before they can communicate through the Netopia R2020. The following illustration shows the minimal requirements for a typical PC or Macintosh computer.



Application software: This is the software you use to send e-mail, browse the World Wide Web, read newsgroups, etc. These applications may require some configuration. Examples include the Eudora e-mail client, and the web browsers Microsoft Internet Explorer and Netscape Navigator.

TCP/IP stack: This is the software that lets your PC or Macintosh communicate using Internet protocols. TCP/IP stacks must be configured with some of the same information you used to configure the Netopia R2020. There are a number of TCP/IP stacks available for PC computers. Windows 95 includes a built-in TCP/IP stack. See "Configuring TCP/IP on Windows 95, 98, or NT computers" on page 3-9. Macintosh computers use either MacTCP or Open Transport. See "Configuring TCP/IP on Macintosh computers" on page 3-13.

Ethernet: Ethernet hardware and software drivers enable your PC or Macintosh computer to communicate on the LAN.

EtherTalk and LocalTalk: These are AppleTalk protocols used over Ethernet.

Once the Netopia R2020 is properly configured and connected to your LAN, PC and Macintosh computers that have their required components in place will be able to connect to the Internet or other remote IP networks.

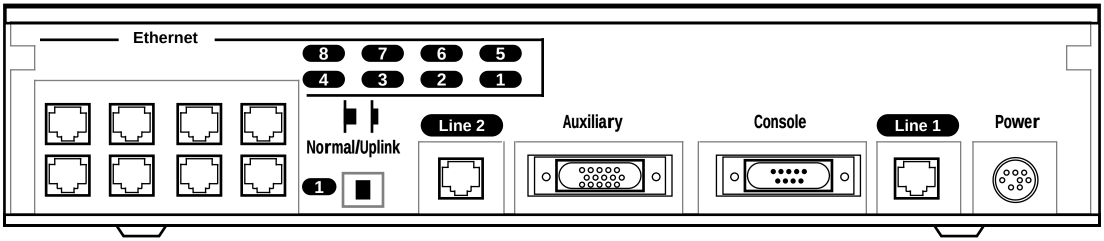
Connecting to an Ethernet network

The Netopia R2020 supports Ethernet connections through its eight Ethernet ports. The Router automatically detects which Ethernet port is in use.

10Base-T

You can connect a standard 10Base-T Ethernet network to the Netopia R2020 using any of its available Ethernet ports.

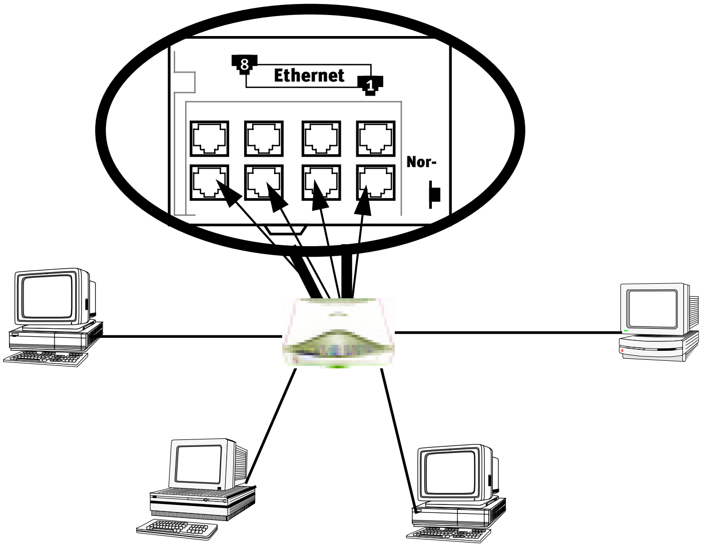
Netopia R2020 back panel



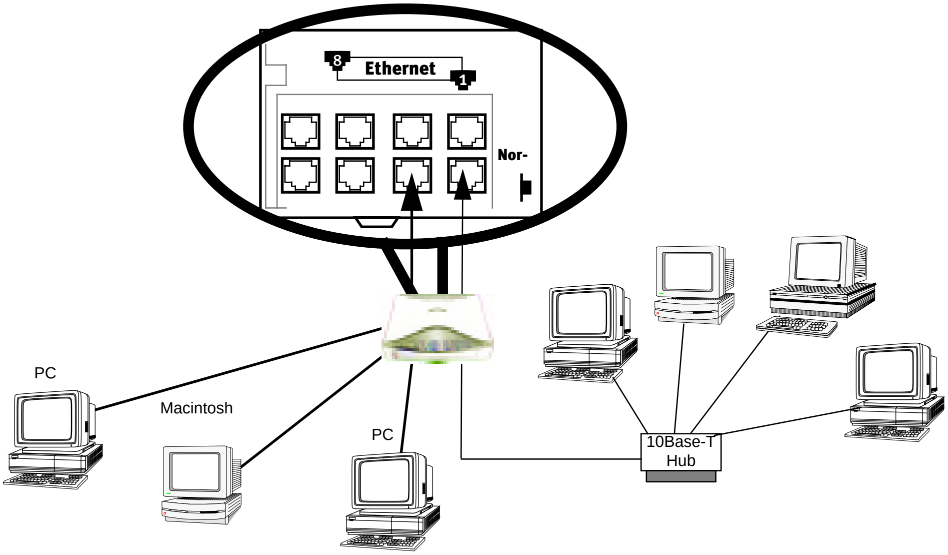
The Netopia R2020 in a 10Base-T network

To connect your 10Base-T network to the Netopia R2020 through an Ethernet port, use a 10Base-T cable with RJ-45 connectors.

If you have more than eight devices to connect, you can attach additional devices using another 10Base-T hub.



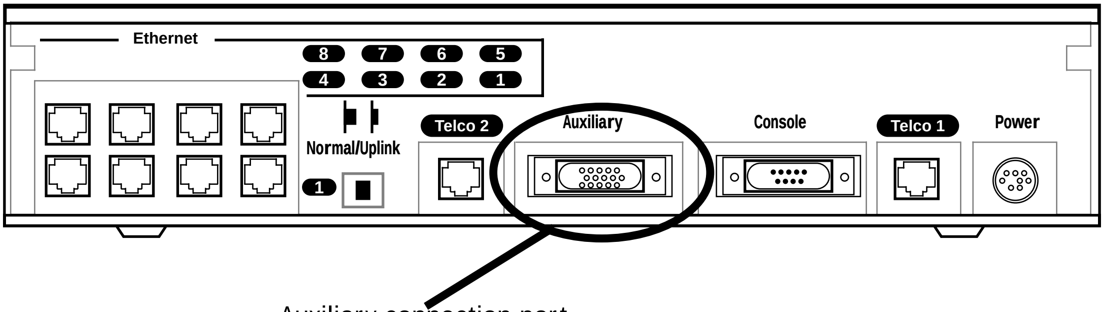
If you add devices connected through a hub, connect the hub to Ethernet port number 1 on the Netopia R2020 and set the Normal/Uplink switch to Uplink.



Adding an external modem

You may wish to add a third (external) modem to gain additional speed for your Internet connection. You will need to obtain the special external modem cable either from your reseller or directly from Netopia. Refer to the sheet of optional feature set add-ons in your Netopia R2020 documentation folio.

Netopia R2020 Auxiliary port for connecting a third modem



Auxiliary connection port
HD-15 (female)

By default, the **Auxiliary** port on your Netopia R2020 is enabled for an external asynchronous modem. This means that all you have to do is connect your modem to the Auxiliary port and configure its settings in the **Line Configuration** screens under the **WAN Configuration** menu. For detailed configuration instructions see "Specifying telephone connections" on page 8-1.

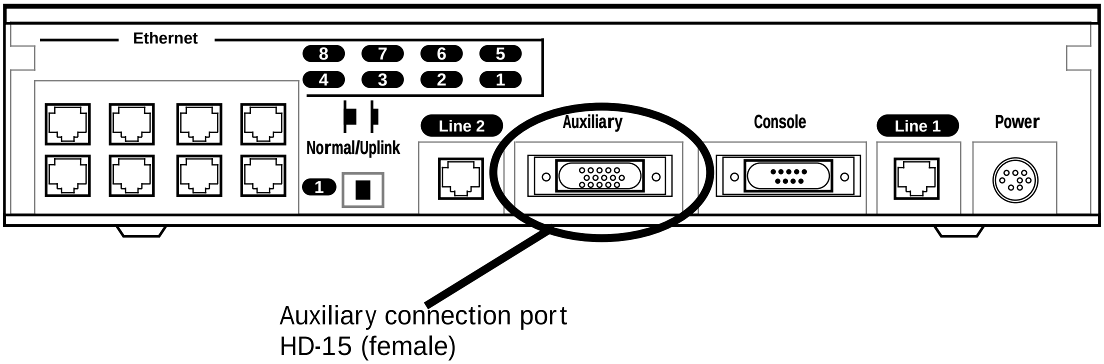
For pinout information on the HD-15 to DB-25 modem cable, see "Pinouts for Auxiliary Port Modem Cable," in Appendix F, "Technical Specifications and Safety Information."

Connecting to a LocalTalk network

If you have purchased the AppleTalk feature expansion kit, you can also connect the Router to an AppleTalk network that uses either Ethernet or LocalTalk. Refer to the sheet of optional feature set add-ons in your Netopia R2020 documentation folio.

The AppleTalk feature expansion kit includes a dual RJ-11 PhoneNET® connector that attaches to the **Auxiliary** port on the Netopia R2020.

Netopia R2020 Auxiliary port for connecting to LocalTalk



Connect the male HD-15 end of the LocalTalk cable to the **Auxiliary** port on your Netopia R2020. Connect the other end of the cable to your LocalTalk network. You can use only one connection on the Auxiliary port. You cannot use both the PhoneNET connector and an external modem.

If your LocalTalk network is not based on standard PhoneNET cabling, use a PhoneNET-to-LocalTalk adaptor cable available from Farallon division of Netopia. Connect the adaptor cable's RJ-11 connector to the AppleTalk cable's PhoneNet connector. Connect the cable's mini-DIN-3 connector to your LocalTalk network.

Be sure to observe the standard rules governing maximum cable lengths and limits on the number of nodes on a PhoneNET network. The dual RJ-11 PhoneNET connector allows insertion in the LocalTalk daisy chain, or at the end. If the device is connected at the end of the daisy chain, you must install the accompanying terminator.

Wiring guidelines for PhoneNET cabling

Topology	22 gauge .642 mm	24 gauge .510 mm	26 gauge .403 mm
daisy chain	n/a	n/a	1800 ft. 549 m
backbone	4500 ft. 1372 m	3000 ft. 229 m	1800 ft. 549 m
4-branch passive star*	1125 ft. 343 m	750 ft. 229 m	450 ft. 137 m
LocalTalk StarController 12-branch active star	3000 ft. 914 m	2000 ft. 610 m	1200 ft. 366 m
* distance is per branch			

For detailed configuration instructions see “AppleTalk Setup” on page 12-1.

Chapter 5

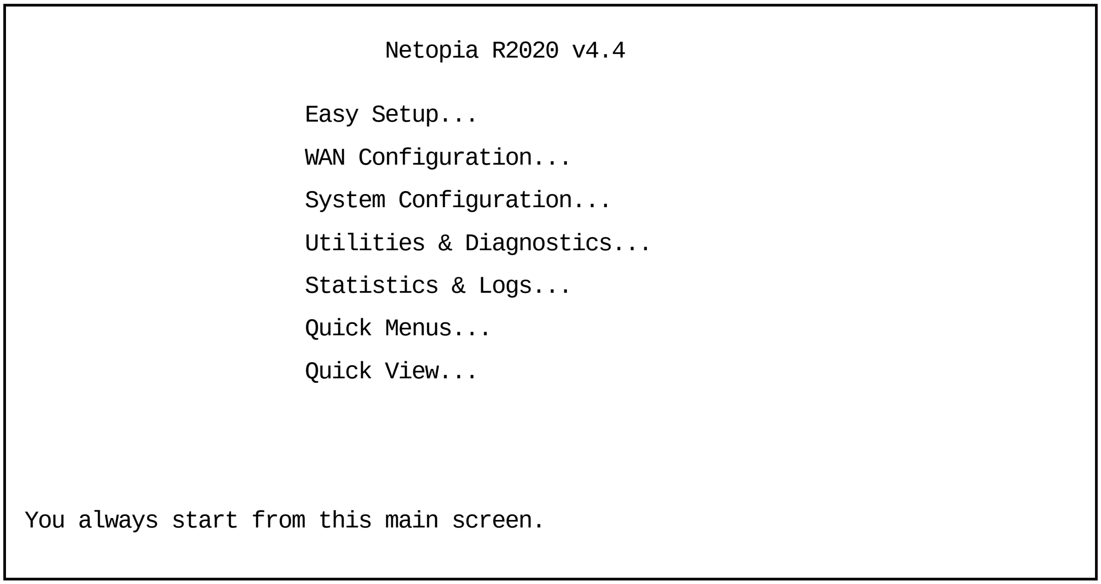
Console-based Management

Console-based management is a menu-driven interface for the capabilities built in to the Netopia R2020. Console-based management provides access to a wide variety of features that the router supports. You can customize these features for your individual setup. This chapter describes how to access and navigate the console-based management screens.

This section covers the following topics:

- "Connecting through a Telnet session" on page 5-2
- "Connecting a local terminal console cable to your router" on page 5-3
- "Navigating through the console screens" on page 5-4

Console-based management screens contain seven entry points to the Netopia Router configuration and monitoring features. The entry points are displayed in the Main Menu shown below:



```
                              Netopia R2020 v4.4

                        Easy Setup...

                        WAN Configuration...

                        System Configuration...

                        Utilities & Diagnostics...

                        Statistics & Logs...

                        Quick Menus...

                        Quick View...




 You always start from this main screen.
```

- The **Easy Setup** menus display and permit changing the values contained in the default Connection Profile you created when you ran the SmartStart Wizard for initial configuration. Experienced users can also use Easy Setup to initially configure the router directly through a console session without using SmartStart.

  Easy Setup menus contain up to five descendant screens for viewing or altering these values. The number of screens depends on whether you have optional features installed.
- The **WAN Configuration** menu displays and permits changing your Connection Profile(s), creating or deleting additional Connection Profiles, and configuring or reconfiguring the manner in which you may be

using the router to connect to more than one service provider or remote site.

- The **System Configuration** menus display and permit changing:
  - Network Protocols Setup. See "Multiple Network Address Translation and IP Setup" on page 10-1.
  - Filter Sets. See "Security" on page 14-1.
  - IP Address Serving. See "IP address serving" on page 10-35.
  - Date and Time. See "Date and Time" on page 7-11.
  - Console Configuration. See "Connecting a local terminal console cable to your router" on page 5-3.
  - SNMP (Simple Network Management Protocol). See "SNMP" on page 13-12.
  - Security. See "Security" on page 14-1.
  - Upgrade Feature Set. See "Upgrade Feature Set" on page 7-12.
  - Logging. See "Logging" on page 7-13.
- The **Utilities & Diagnostics** menus provide a selection of tools for monitoring and diagnosing the router's behavior, as well as updating the firmware and rebooting the system. See "Utilities and Diagnostics" on page 15-1 for detailed information.
- The **Statistics & Logs** menus display several sets of tables and device logs that show information about your router, your network and their history. See "Statistics & Logs" on page 13-4 for detailed information.
- The **Quick Menus** screen is a shortcut entry point to the most commonly used configuration menus that are accessed through the other menu entry points.
- The **Quick View** menu displays at a glance current real-time operating information about your router. See "Quick View status overview" on page 13-1 for detailed information.

Connecting through a Telnet session

Features of the Netopia R2020 may be configured through the console screens.

Before you can access the console screens through Telnet, you must have:

- a network connection locally to the router or IP access to the router through the WAN port. This could be the same connection as the one you used with SmartStart.

  Note: Alternatively, you can have a direct serial console cable connection using the provided console cable for your platform (PC or Macintosh) and the "Console" port on the back of the router. For more information on attaching the console cable, see "Connecting a local terminal console cable to your router" on page 5-3.
- **Telnet** software installed on the computer you will use to configure the router

Configuring Telnet software

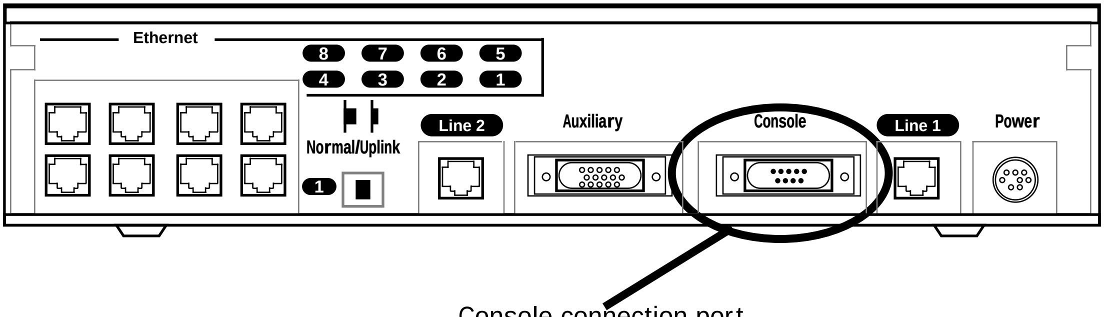
If you are configuring your router using a Telnet session, your computer must be running a Telnet software program.

- If you connect a PC with Microsoft Windows, you can use a Windows Telnet application or simply run Telnet from the Start menu.
- If you connect a Macintosh computer, you can use the NCSA Telnet program supplied on the Netopia R2020 CD. You install NCSA Telnet by simply dragging the application from the CD to your hard disk.

Connecting a local terminal console cable to your router

You can perform all of the System Configuration activities for your Netopia R2020 through a local serial console connection using terminal emulation software, such as HyperTerminal provided with Windows95 on the PC, or ZTerm, included on the Netopia CD, for the Macintosh.

The Netopia R2020 back panel has a connector labeled "Console" for attaching the Router to either a PC or Macintosh computer via the serial port on the computer. (On a Macintosh, the serial port is called the Modem port or the Printer port.) This connection lets you use the computer to configure and monitor the Netopia R2020 via the console screens.



Console connection port
DE-9 (male)

To connect the Netopia R2020 to your computer for serial console communication, use the supplied dual console cable connector end appropriate to your platform:

- one DE-9 connector end attaches to a PC
- the mini-DIN8 connector end attaches to a Macintosh
- the DE-9 end of the Console cable attaches to the Netopia R2020's Console port

If you are configuring your router via a *terminal* session, your computer must be running a standard terminal emulation or communications software program, such as those used with modems.

- If you connect a PC with Microsoft Windows 95 or NT, you can use the HyperTerminal application bundled with the operating system.
- If you connect a Macintosh computer, you can use the ZTerm terminal emulation program on the supplied Netopia R2020 CD.

Launch your terminal emulation software and configure the communications software for the following values. These are the default communication parameters that the Netopia R2020 uses.

Parameter	Suggested Value
Terminal type	**PC**: ANSI, VT100 **Mac**: ANSI, VT-100, or VT-200
Data bits	8
Parity	None
Stop bits	1
Speed	Options are: 9600, 19200, 38400, or 57600 bits per second
Flow Control	None
Note: The router firmware contains an autobaud detection feature. If you are at any screen on the serial console, you can change your baud rate and press Return (HyperTerminal for the PC requires a disconnect). The new baud rate is displayed at the bottom of the screen.	

Navigating through the console screens

Use your keyboard to navigate the Netopia R2020's configuration screens, enter and edit information, and make choices. The following table lists the keys to use to navigate through the console screens.

To...	Use These Keys...
Move through selectable items in a screen or pop-up menu	Up, Down, Left, and Right Arrow
To set a change to a selected item or open a pop-up menu of options for a selected item like entering an upgrade key	Return or Enter
Change a toggle value (Yes/No, On/Off)	Tab
Restore an entry or toggle value to its previous value	Esc
Move one item up	Up arrow or Control + k
Move one item down	Down arrow or Control + j
Display a dump of the device event log	Control + e
Display a dump of the WAN event log	Control + f
Refresh the screen	Control + L
Go to topmost selectable item	<
Go to bottom right selectable item	>

Chapter 6

Easy Setup

This chapter describes how to use the Easy Setup console screens on your Netopia R2020 Dual Analog Router. The Easy Setup console screens provide an alternate method for experienced users to set up their router's Connection Profiles without using SmartStart. After completing the Easy Setup console screens, your router will be ready to connect to the Internet or another remote site.

Easy Setup console screens

Using three Easy Setup console screens, you can:

- modify a Connection Profile for your Router for the connection to your ISP or remote location;
- set up IP addresses and IP address serving;
- password protect configuration access to your Netopia R2020 Dual Analog Router;

How to access the Easy Setup console screens

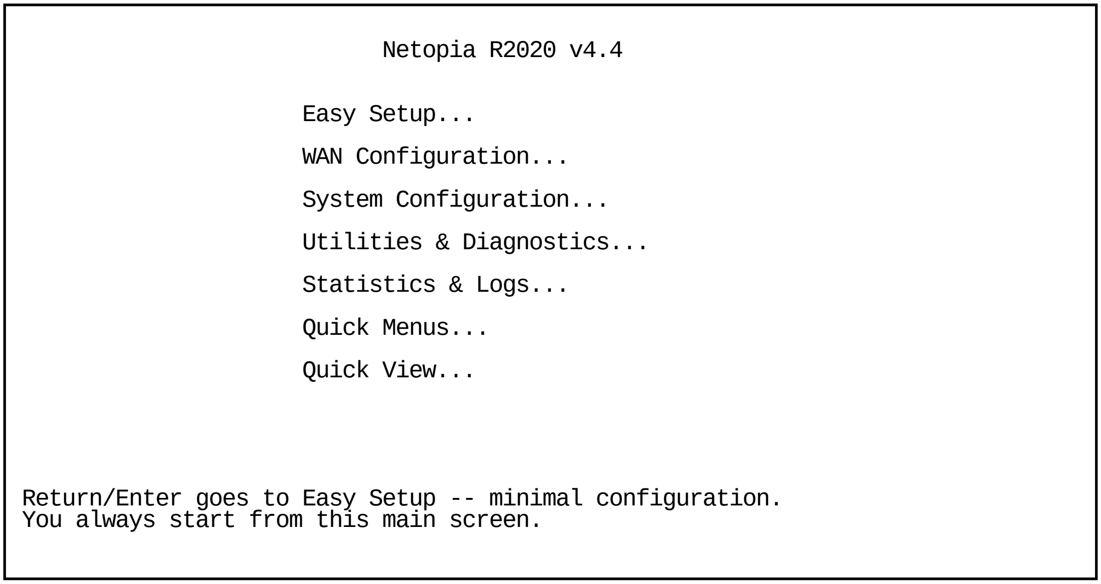
To access the console screens, Telnet to the Netopia Router over your Ethernet network, or you can physically connect with a serial console cable and access the Netopia Router with a terminal emulation program. See "Connecting through a Telnet session" on page 5-2 or "Connecting a local terminal console cable to your router" on page 5-3.

Note: Before continuing, make sure that you have the information that your telephone service provider, ISP, or network administrator has given you to configure the Netopia Router.

The Netopia Router's first console screen, Main Menu, appears in the terminal emulation window of the attached PC or Macintosh when:

- the Netopia Router is turned on
- the computer is connected to the Netopia Router
- the Telnet or terminal emulation software is running and configured correctly.

A screen similar to the following appears:



```
                             Netopia R2020 v4.4

                       Easy Setup...

                       WAN Configuration...

                       System Configuration...

                       Utilities & Diagnostics...

                       Statistics & Logs...

                       Quick Menus...

                       Quick View...




Return/Enter goes to Easy Setup -- minimal configuration.
You always start from this main screen.
```

If you do not see the Main Menu, verify that:

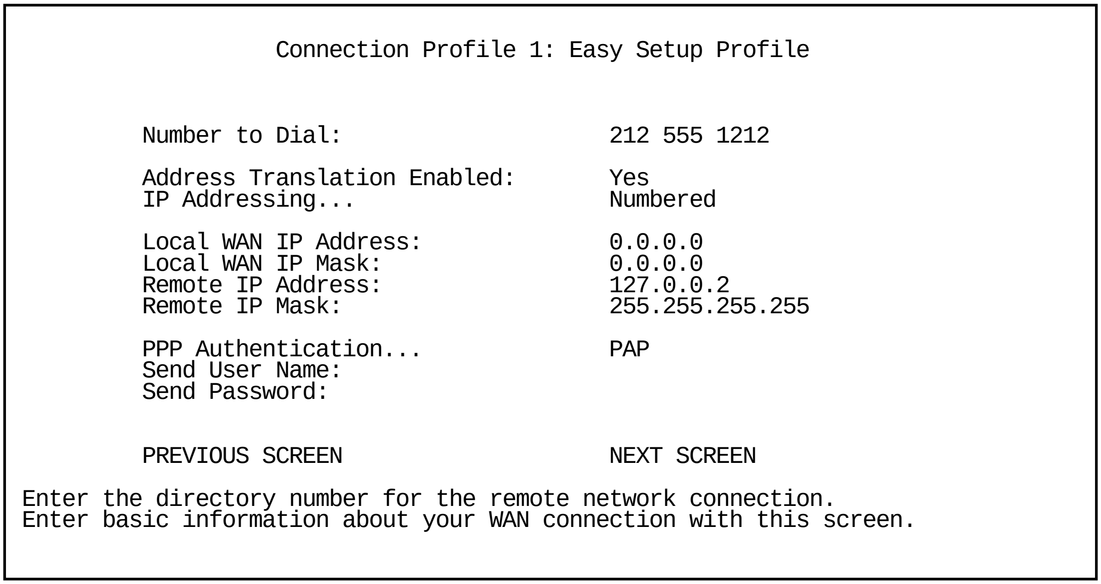
- the computer used to view the console screen has its serial port connected to the Netopia R2020's "Console" port or an Ethernet connection to one of its Ethernet ports. See "Connecting a local terminal console cable to your router" on page 5-3 or "Connecting through a Telnet session" on page 5-2.
- the Telnet or terminal emulation software is configured for the recommended values.
- if you are connecting via the Console port, the console's serial port is not being used by another device, such as an internal modem, or an application. Turn off all other programs (other than your terminal emulation program) that may be interfering with your access to the port.
- you have entered the correct password, if necessary. Your Netopia R2020's console access may be password protected from a previous configuration. See your system administrator to obtain the password.

  See Appendix A, "Troubleshooting," for more suggestions.

Beginning Easy Setup

To begin Easy Setup, select **Easy Setup** in the Main Menu, then press Return.

The Easy Setup Profile screen appears.



```
                    Connection Profile 1: Easy Setup Profile


          Number to Dial:                   212 555 1212

          Address Translation Enabled:      Yes
          IP Addressing...                  Numbered

          Local WAN IP Address:             0.0.0.0
          Local WAN IP Mask:                0.0.0.0
          Remote IP Address:                127.0.0.2
          Remote IP Mask:                   255.255.255.255

          PPP Authentication...             PAP
          Send User Name:
          Send Password:


          PREVIOUS SCREEN                   NEXT SCREEN

 Enter the directory number for the remote network connection.
 Enter basic information about your WAN connection with this screen.
```

Easy Setup profile

The Easy Setup Profile screen is where you configure the parameters that control the Netopia R2020's connection to a specific remote destination, usually an ISP or a corporate site.

On a Netopia R2020 Dual Analog Router you can add up to 15 more connection profiles, for a total of 16. See "Creating a new Connection Profile" on page 7-2.

1. Select **Number to Dial** and enter the telephone number you received from your ISP. This is the number the Netopia R2020 dials to reach your ISP. Enter the number as you would dial it, including any required prefixes (such as area, access, and long-distance dialing codes). You may also use punctuation.

   Note: When placing a multi-channel call, the answering equipment must either:

   - be in a "hunt group," where a single telephone number services multiple lines, or
   - the answering side must implement MP or BAP as a method to advise the calling side what number(s) to use.

   ISPs or corporate IS groups will meet these conditions. For other non-standard dialup connections, you should verify that one or the other of these conditions is true.

2. To enable address translation, toggle **Address Translation Enabled** to **Yes**. For more information on Network Address Translation, see "Multiple Network Address Translation and IP Setup" on page 10-1.

3. Select **IP Addressing** and press Return. From the pop-up menu choose Numbered or Unnumbered (the default).

4. Select **Local WAN IP Address** and enter the local WAN address your ISP gave you.

   The default address is 0.0.0.0, which allows for dynamic addressing, when your ISP assigns an address each time you connect. However, you may enter another address if you want to use static addressing.

   - When using numbered interfaces, the Netopia Router will use its local WAN IP address and subnet mask to send packets to the remote router. Both routers have WAN IP addresses and subnet masks associated with the connection.
   - When using unnumbered interfaces, the Netopia Router will use either its local Ethernet IP address or its NAT address (if so configured) and subnet mask to send packets to the remote router. Neither router has a WAN IP address or subnet mask associated with this connection.

   Note: If your ISP has not given you their IP or subnet mask addresses, then you can enter an IP address such as 127.0.0.2, and an IP subnet mask such as 255.0.0.0. With these settings the router will get this information dynamically when it connects to the remote site.

5. If your ISP uses unnumbered (system-based routing), select **Remote IP Address** and enter the IP address your ISP gave you.

   Then select **Remote IP Mask** and enter the IP subnet mask of the remote site you will connect to.

6. Select the **PPP Authentication** pop-up menu and choose the type of connection security your ISP told you to use (**PAP**, **CHAP**, **PAP-TOKEN**, or **CACHE-TOKEN**). If you choose any of these authentication methods, go to the next step. If your ISP does not use any of these authentication methods, choose **None** and skip to the last step. When you create a connection profile from Easy Setup, the default setting is PAP.

7. If your ISP uses PAP or PAP-TOKEN, select **Send User Name** and enter the user name your ISP gave you to connect. If you selected PAP, select **Send Password** and enter your password. If you selected PAP-TOKEN, you don't enter the password now. Your name and password can be up to 32 characters each.

   If your ISP uses CHAP, select **Send Host Name** and enter the user name your ISP gave you to connect. Then select **Send Secret** and enter the secret (CHAP term for password) your ISP gave you.

   If your ISP uses CACHE-TOKEN, select **Send User Name** and enter the user name your ISP gave you to connect. Select **Send Password** and enter your password.

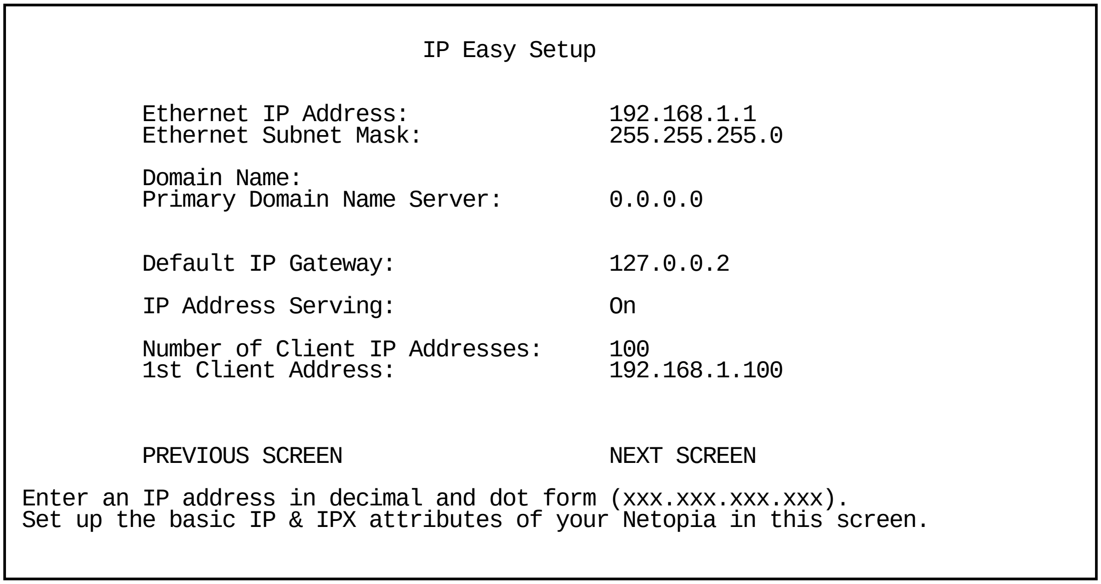
8. Select **NEXT SCREEN** and press Return. The IP Easy Setup screen appears.

IP Easy Setup

The IP Easy Setup screen is where you enter information about your Netopia Router's:

- IP address
- Subnet mask
- Default gateway IP address
- Domain name server IP address
- IP address serving information, such as the number of client IP addresses and the 1st client address

You should consult with your network administrator to obtain the information you will need. For more information about setting up IP, see "Multiple Network Address Translation and IP Setup" on page 10-1.



```
                         IP Easy Setup

         Ethernet IP Address:               192.168.1.1
         Ethernet Subnet Mask:              255.255.255.0

         Domain Name:
         Primary Domain Name Server:        0.0.0.0


         Default IP Gateway:                127.0.0.2

         IP Address Serving:                On

         Number of Client IP Addresses:     100
         1st Client Address:                192.168.1.100



         PREVIOUS SCREEN                    NEXT SCREEN

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
Set up the basic IP & IPX attributes of your Netopia in this screen.
```

1. Select **Ethernet IP Address** and enter the first IP address from the IP address range your ISP has given you. This will be the Netopia Router's IP address.

   If Network Address Translation is enabled in the Easy Setup connection profile, the Ethernet IP Address defaults to an address within a range reserved by the Internet address administration authority for use within private networks, 192.168.1.1.

   Because this is a private network address, it should never be directly connected to the Internet. Using NAT for all your connection profiles will ensure this restriction. See "Multiple Network Address Translation and IP Setup" on page 10-1 of this guide for more information.

2. Select **Ethernet Subnet Mask** and enter the subnet mask your ISP has given you. The **Ethernet Subnet Mask** defaults to a standard class C mask (for unlimited user models; smaller, for restricted user models).
3. Select **Domain Name** and enter the domain name your ISP has given you.
4. Select **Primary Domain Name Server** and enter the IP address your ISP has given you.
5. The **Default IP Gateway** defaults to the remote IP address you entered in the Easy Setup connection profile. If the Netopia Router does not recognize the destination of any IP traffic, it forwards that traffic to this gateway.

   Do not confuse the remote IP address and the default gateway's IP address with the block of local IP addresses you receive from your ISP. You use the local IP addresses for the Netopia R2020's Ethernet port and for IP clients on your local network. The remote IP address and the default gateway's IP address should point to your ISP's router.

6. To use DHCP and (if installed) MacIP address serving, toggle **IP Address Serving** to **On**.

   Note: For information about dynamic IP address serving, see "Multiple Network Address Translation and IP Setup" on page 10-1.

7. If **IP Address Serving** is **On**, select **Number of Client IP Addresses**. Then enter the number of available host addresses for the Netopia R2020 Dual Analog Router to allocate to the client computers on your network. This number defaults to the balance of the subnet addresses above the Netopia Router's address.

8. If **IP Address Serving** is **On**, select **1st Client Address** and enter the first IP address in the set of allocated served IP addresses.

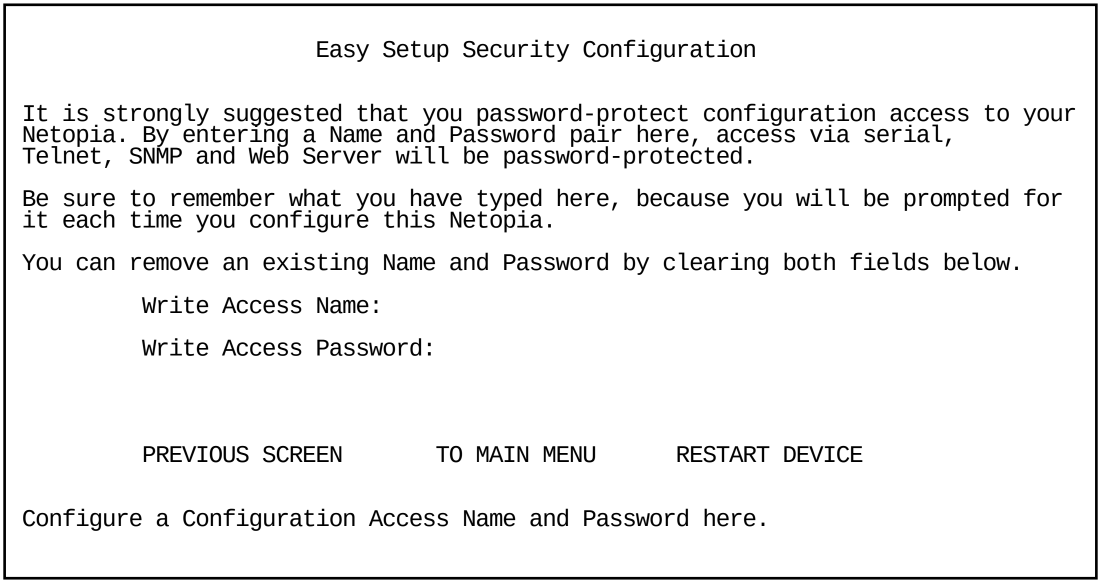
9. Press Return. The Easy Setup Security Configuration screen appears.

Easy Setup Security

The Easy Setup Security Configuration screen lets you password-protect your Netopia R2020. Input your Write Access Name and Write Access Password with names or numbers totaling up to eleven digits.

If you password protect the console screens, you will be prompted to enter the name and password you have specified every time you log in to the console screens. Do not forget your name and password. If you do, you will be unable to access any of the configuration screens.

Additional security features are available. See "Security" on page 14-1.



```
                       Easy Setup Security Configuration


It is strongly suggested that you password-protect configuration access to your
Netopia. By entering a Name and Password pair here, access via serial,
Telnet, SNMP and Web Server will be password-protected.

Be sure to remember what you have typed here, because you will be prompted for
it each time you configure this Netopia.

You can remove an existing Name and Password by clearing both fields below.

         Write Access Name:

         Write Access Password:



         PREVIOUS SCREEN       TO MAIN MENU      RESTART DEVICE


Configure a Configuration Access Name and Password here.
```

The final step in configuring the Easy Setup console screens is to restart the Netopia R2020, so the configuration settings take effect.

1. Select **RESTART DEVICE**. A prompt asks you to confirm your choice.

2. Select **CONTINUE** to restart the Netopia Router and have your selections take effect.

Note: You can also restart the system at any time by using the restart utility (see "Restarting the system" on page 15-13) or by turning the Netopia Router off and on with the power switch.

Easy Setup is now complete.

Part II: Advanced Configuration

Chapter 7

WAN and System Configuration

This chapter describes how to use the console-based management screens to access and configure advanced features of your Netopia R2020 Dual Analog Router. You can customize these features for your individual setup. These menus provide a powerful method for experienced users to set up their router's connection profiles and system configuration.

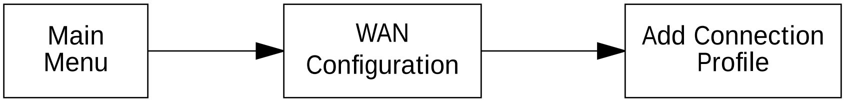
The next chapter "Managing Data Calls" on page 8-1 explains more of the Netopia R2020's special features for cost control and dial-in connections.

This section covers the following topics:

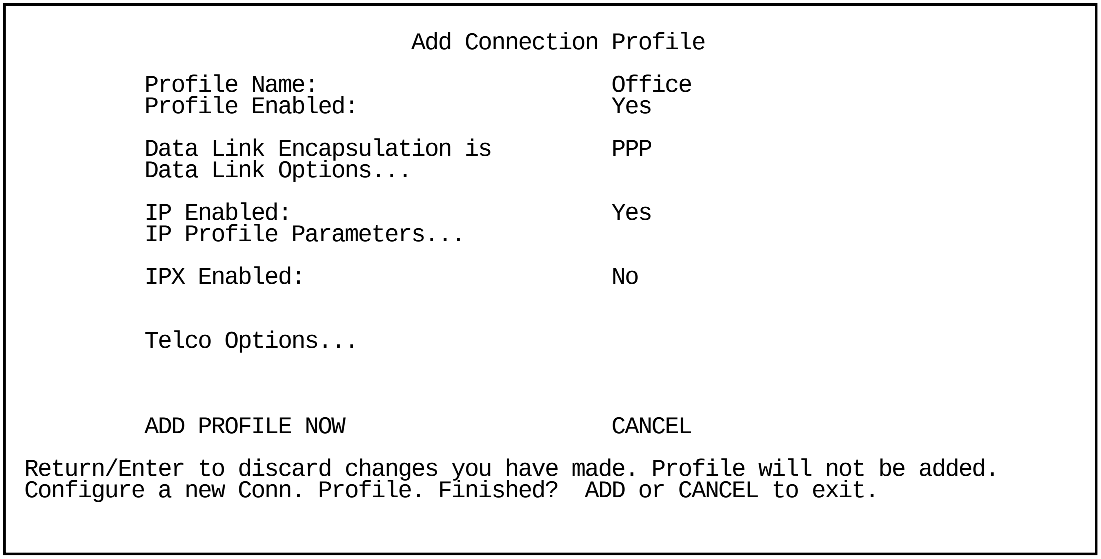
- "Creating a new Connection Profile" on page 7-2
- "System Configuration screens" on page 7-7
- "Navigating through the System Configuration screens" on page 7-8
- "System Configuration features" on page 7-8

Creating a new Connection Profile

Connection Profiles define the telephone and networking protocols necessary for the router to make a remote connection. A Connection Profile is like an address book entry describing how the router is to get to a remote site, or how to recognize and authenticate a remote user dialing in to the router. For example, to create a new **Connection Profile**, you navigate to the **WAN Configuration** screen from the Main Menu, and select Add Connection Profile.



The **Add Connection Profile** screen appears.



```
                              Add Connection Profile

          Profile Name:                      Office
          Profile Enabled:                   Yes

          Data Link Encapsulation is         PPP
          Data Link Options...

          IP Enabled:                        Yes
          IP Profile Parameters...

          IPX Enabled:                       No


          Telco Options...



          ADD PROFILE NOW                    CANCEL

 Return/Enter to discard changes you have made. Profile will not be added.
 Configure a new Conn. Profile. Finished?  ADD or CANCEL to exit.
```

On a Netopia R2020 Dual Analog Router you can add up to 15 more connection profiles, for a total of 16.

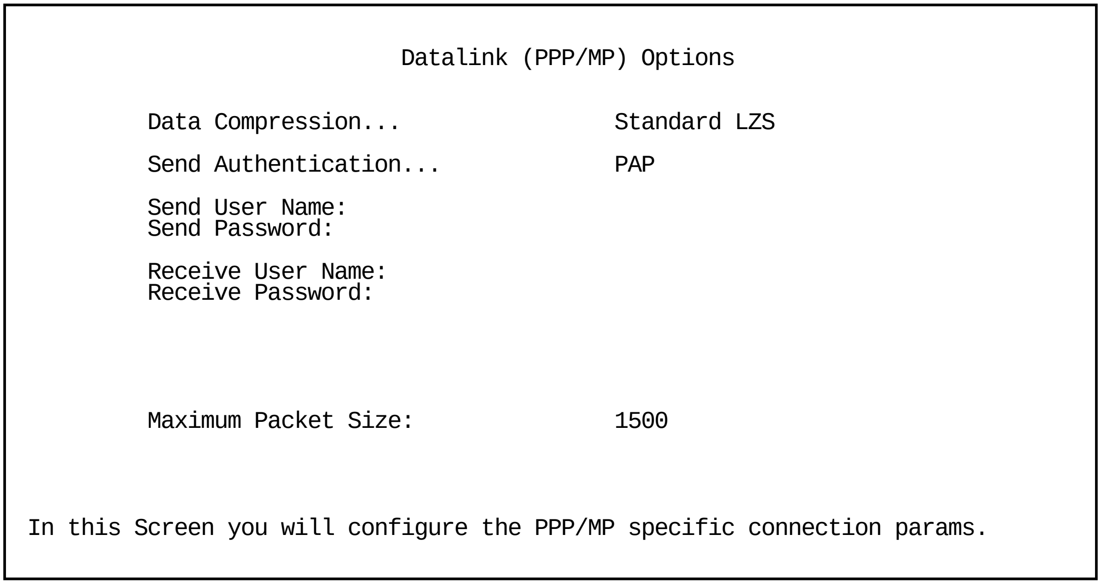
1. Select **Profile Name** and enter a name for this connection profile. It can be any name you wish. For example: the name of your ISP.

2. Toggle the **Profile Enabled** value to Yes or No. The default is Yes.

3. If you are creating a Virtual Private Network (VPN) profile (see "Virtual Private Networks" on page 9-1), you can choose either PPTP or ATMP from the **Data Link Encapsulation** pop-up menu. Otherwise, accept the default PPP.

4. Select **Datalink Options** and press Return. The Datalink Options screen appears.

   Note: The Datalink Options shown below are for the default Data Link Encapsulation method PPP. (For VPN Data Link Options see "Virtual Private Networks" on page 9-1.)



```
                      Datalink (PPP/MP) Options

         Data Compression...                 Standard LZS

         Send Authentication...              PAP

         Send User Name:
         Send Password:

         Receive User Name:
         Receive Password:



         Maximum Packet Size:                1500



In this Screen you will configure the PPP/MP specific connection params.
```

   You can accept the defaults, or change them if you wish.

   Data Compression options are: Ascend LZS, Standard LZS (the default), or None.

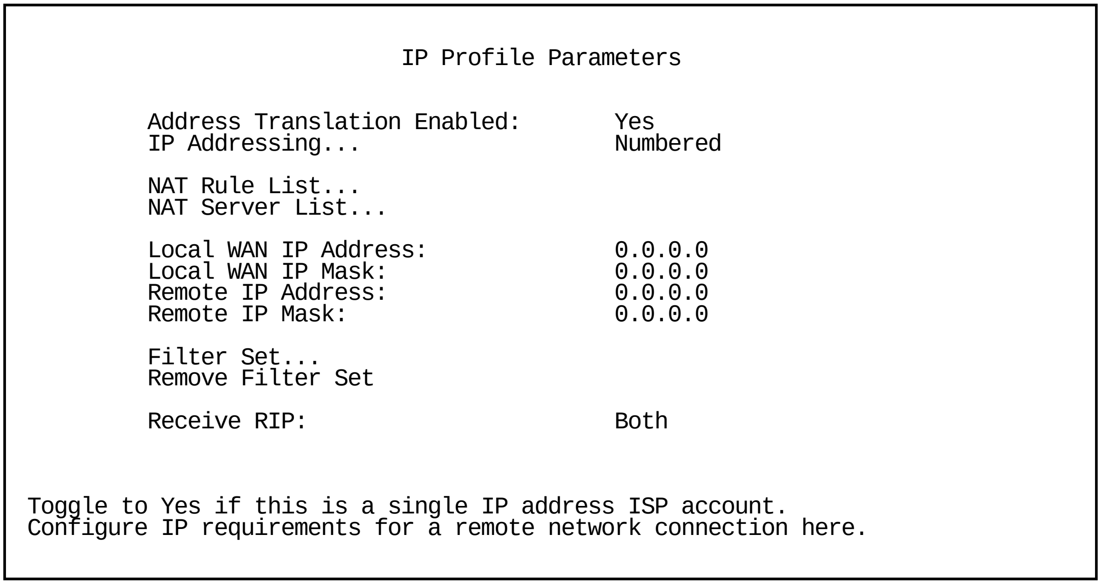
   Send Authentication options are: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), the secure token protocols PAP-TOKEN and CACHE-TOKEN, or None, the default. For more information about token security see "Token Security Authentication" on page 14-36. If your ISP does not use any of these authentication methods, choose None. The Send Authentication information is used to authenticate your call to your service provider. The **Receive User Name** and **Password** information is used to authenticate attempted dial-in connections.

   - If your ISP uses PAP or PAP-TOKEN, select **Send User Name** and enter the user name your ISP gave you to connect. If you selected PAP, select **Send Password** and enter your password. If you selected PAP-TOKEN, you don't enter the password now.
   - If your ISP uses CHAP, select **Send Host Name** and enter the user name your ISP gave you to connect. Then select **Send Secret** and enter the secret (CHAP term for password) your ISP gave you.
   - If your ISP uses CACHE-TOKEN, select **Send User Name** and enter the user name your ISP gave you to connect. Select **Send Password** and enter your password.

     You can specify user name and password for both outgoing and incoming calls. Your name and password can be up to 32 characters each.
   - Enter a **Maximum Packet Size** between 128 and 1510 bytes. 1500 is the default.

   Return to the Add Connection Profile screen by pressing Escape.

5. Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

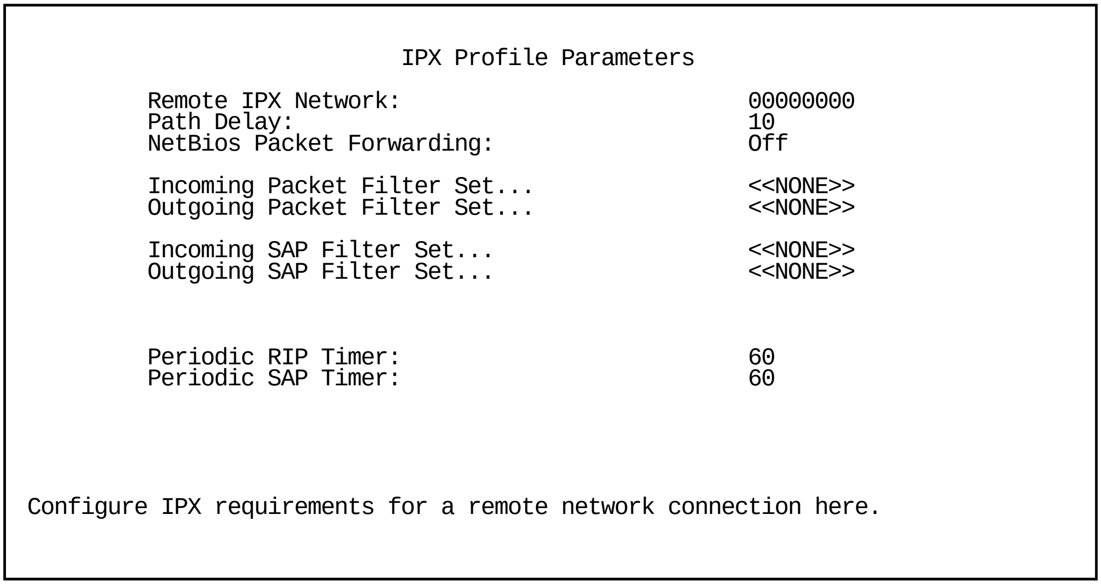


```
                          IP Profile Parameters

         Address Translation Enabled:       Yes
         IP Addressing...                   Numbered

         NAT Rule List...
         NAT Server List...

         Local WAN IP Address:              0.0.0.0
         Local WAN IP Mask:                 0.0.0.0
         Remote IP Address:                 0.0.0.0
         Remote IP Mask:                    0.0.0.0

         Filter Set...
         Remove Filter Set

         Receive RIP:                       Both


Toggle to Yes if this is a single IP address ISP account.
Configure IP requirements for a remote network connection here.
```

6. Toggle or enter any IP Parameters you require and return to the Add Connection Profile screen by pressing Escape. For more information, see "Multiple Network Address Translation and IP Setup" on page 10-1.

7. If you will be connecting with an IPX remote network, toggle **IPX Enabled** to Yes, and press Return. Otherwise, accept the default No.

   If you enable IPX routing, an **IPX Profile Parameters** menu item becomes available. Select IPX Profile Parameters and press Return. The IPX Profile Parameters screen appears.

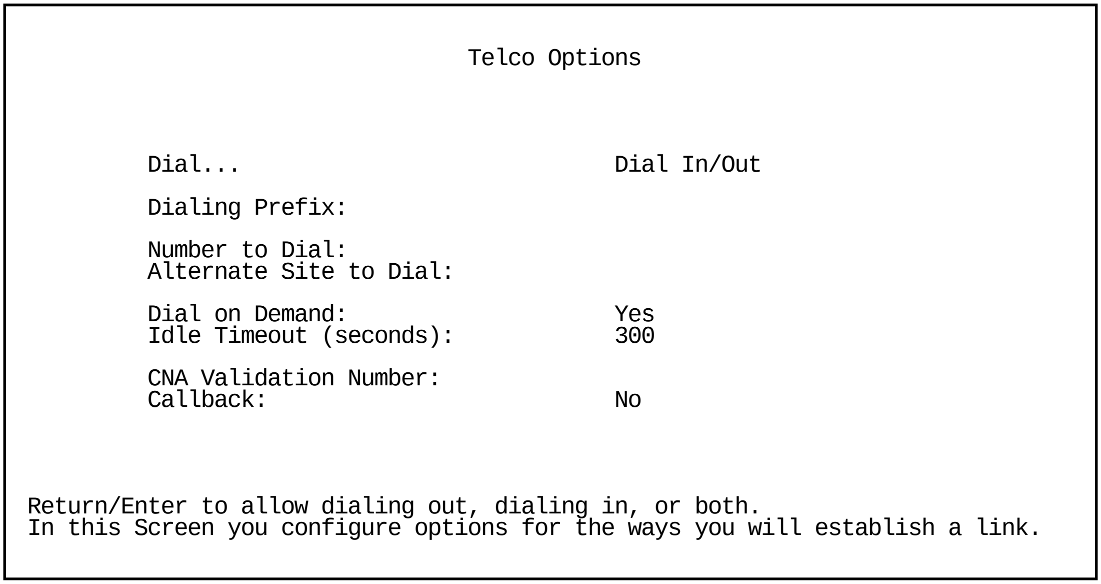


```
                          IPX Profile Parameters

         Remote IPX Network:                          00000000
         Path Delay:                                  10
         NetBios Packet Forwarding:                   Off

         Incoming Packet Filter Set...                <<NONE>>
         Outgoing Packet Filter Set...                <<NONE>>

         Incoming SAP Filter Set...                   <<NONE>>
         Outgoing SAP Filter Set...                   <<NONE>>


         Periodic RIP Timer:                          60
         Periodic SAP Timer:                          60



Configure IPX requirements for a remote network connection here.
```

8. Toggle or enter any IPX Parameters you require and return to the Add Connection Profile screen by pressing Escape. For more information, see "IPX Setup" on page 11-1.

9. Select **Telco Options** and press return. the Telco Options screen appears.

   NOTE: If you are creating a VPN Connection Profile, the Telco Options menu is not used and becomes unavailable.



```
                                Telco Options



           Dial...                          Dial In/Out

           Dialing Prefix:

           Number to Dial:
           Alternate Site to Dial:

           Dial on Demand:                  Yes
           Idle Timeout (seconds):          300

           CNA Validation Number:
           Callback:                        No



  Return/Enter to allow dialing out, dialing in, or both.
  In this Screen you configure options for the ways you will establish a link.
```

   Select **Dial** and press Return. A pop-up menu appears. You can select the dialing options for this Connection Profile as Dial In Only, Dial Out Only, or Dial In/Out.

   You can:

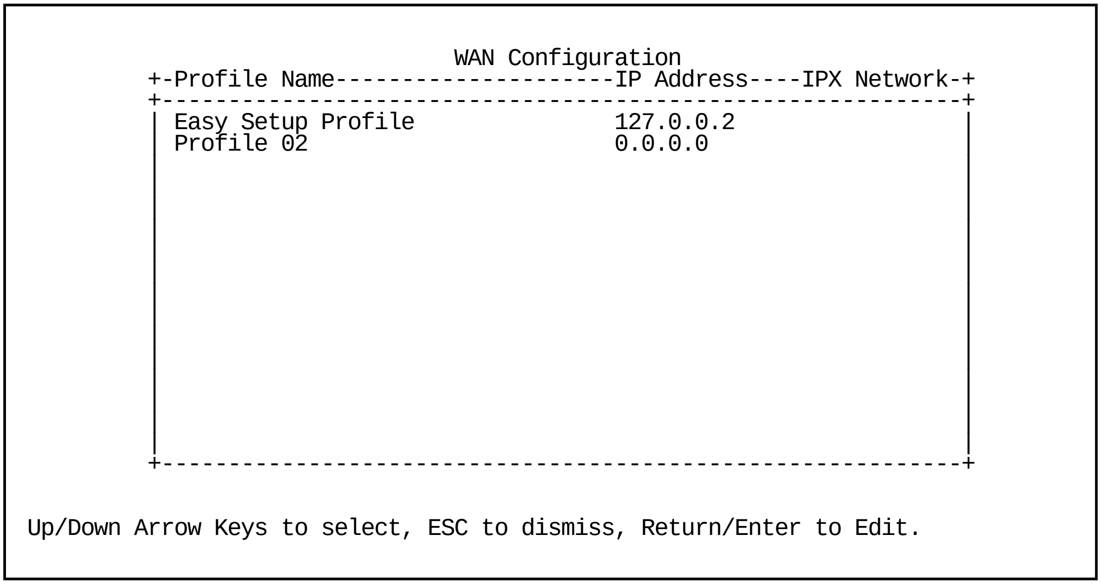
   - add a dialing prefix, such as “9” for an outside line on a PBX or Centrex phone system.
   - add the number to dial for this Connection Profile
   - add an alternate number to use if the first number fails to connect
   - change any of the default parameter settings

   When you are finished with these entries, press Escape to return to the **Add Connection Profile** screen.

10. Select **ADD PROFILE NOW** and press Return. Your new Connection Profile will be added.

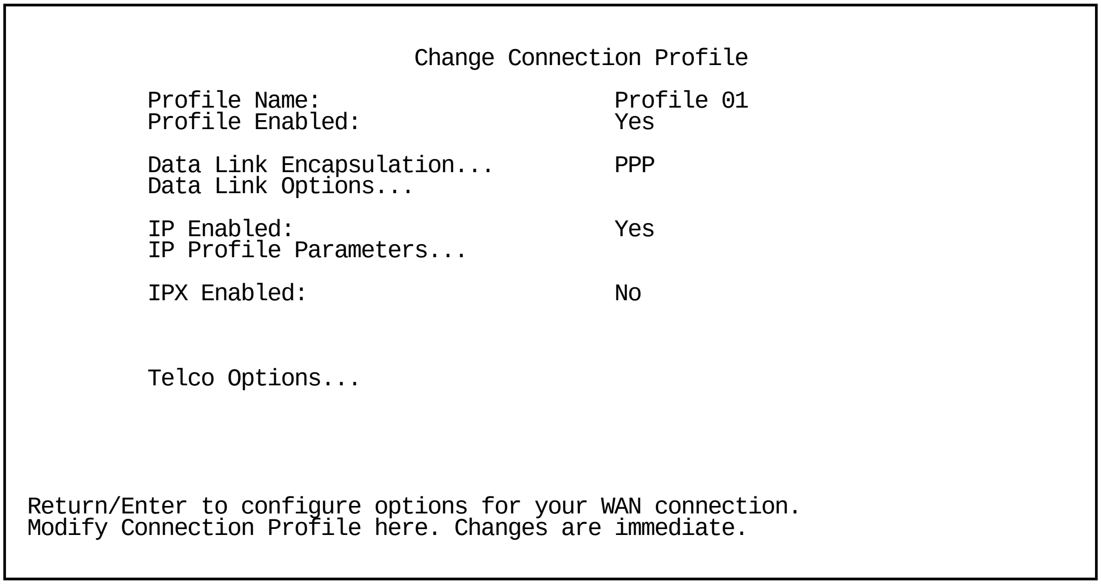
Viewing or editing connection profiles

If you want to view or edit the connection profiles in your router, return to the WAN Configuration screen, and select **Display/Change Connection Profile**. The list of Connection Profiles is displayed in a scrolling pop-up screen.



```
                           WAN Configuration
          +-Profile Name---------------------IP Address----IPX Network-+
          +------------------------------------------------------------+
          | Easy Setup Profile               127.0.0.2                  |
          | Profile 02                       0.0.0.0                    |
          |                                                             |
          |                                                             |
          |                                                             |
          |                                                             |
          |                                                             |
          |                                                             |
          |                                                             |
          |                                                             |
          |                                                             |
          |                                                             |
          |                                                             |
          |                                                             |
          |                                                             |
          +------------------------------------------------------------+


 Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

Select the connection profile you want to view or edit and press Return. The profile is displayed, and you can change any of the parameters. Changes take effect immediately without rebooting the router.

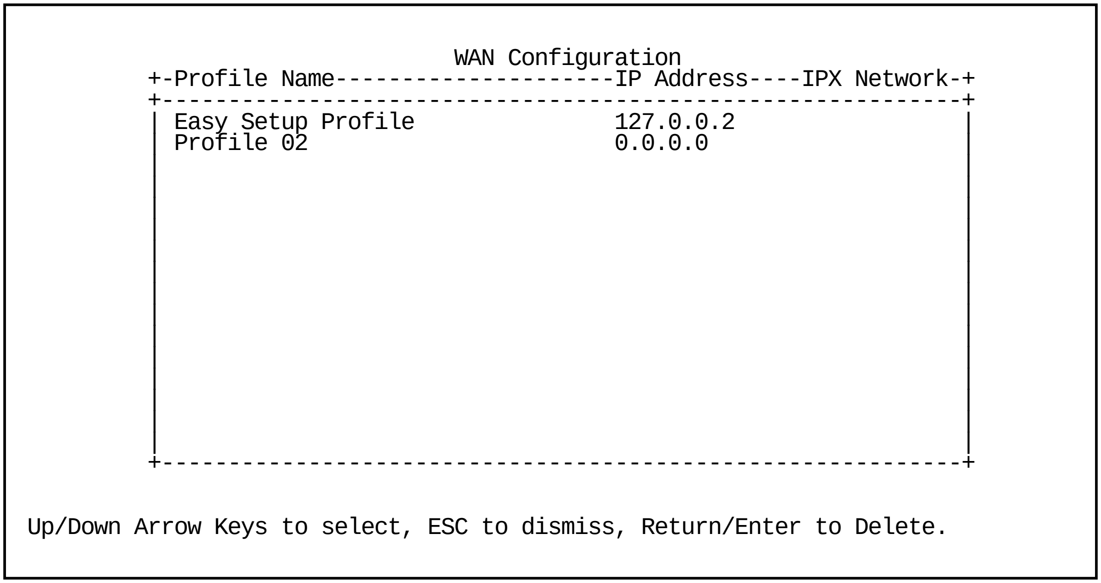


```
                        Change Connection Profile

          Profile Name:                      Profile 01
          Profile Enabled:                   Yes

          Data Link Encapsulation...         PPP
          Data Link Options...

          IP Enabled:                        Yes
          IP Profile Parameters...

          IPX Enabled:                       No



          Telco Options...





 Return/Enter to configure options for your WAN connection.
 Modify Connection Profile here. Changes are immediate.
```

Deleting connection profiles

You can delete a connection profile by returning to the WAN Configuration menu and selecting **Delete Connection Profile**.

A scrolling pop-up screen appears. Select the profile you want to delete and press Return. When prompted, select **CONTINUE**, and the connection profile will be deleted.



```
                                WAN Configuration
         +-Profile Name---------------------IP Address----IPX Network-+
         +------------------------------------------------------------+
         | Easy Setup Profile               127.0.0.2                 |
         | Profile 02                       0.0.0.0                   |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         |                                                            |
         +------------------------------------------------------------+


Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Delete.
```

System Configuration screens

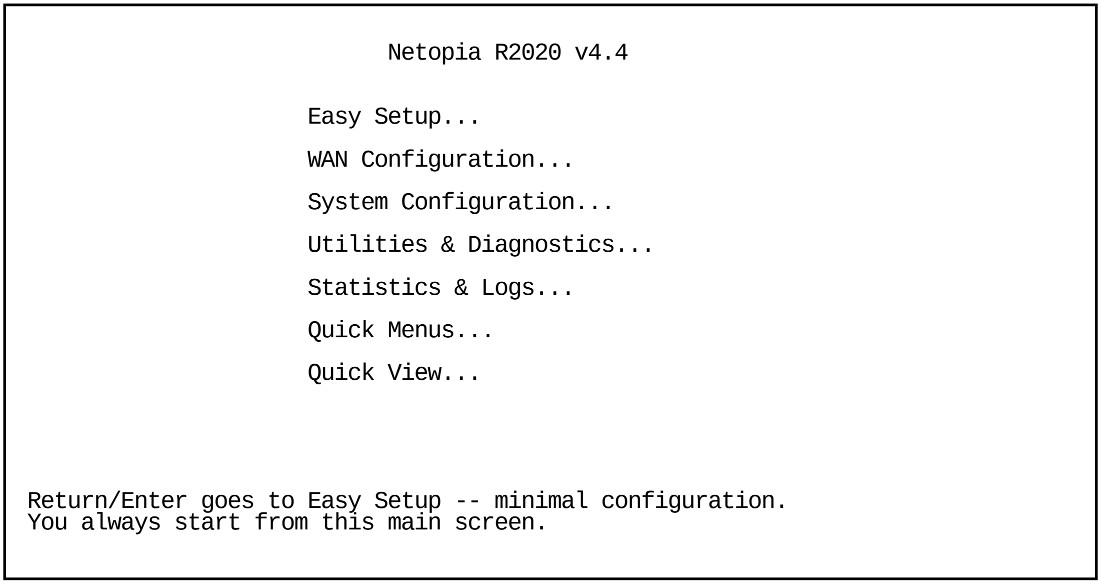
You can connect to the Netopia R2020’s System Configuration screens:

- Using Telnet with the Router’s Ethernet port IP address
- Through the console port, using a local terminal (see “Connecting a local terminal console cable to your router” on page 5-3)

You can also retrieve the Netopia R2020’s configuration information and remotely set its parameters using the Simple Network Management Protocol (see “SNMP” on page 13-12).

Open a Telnet connection to the IP address you set in the router with SmartStart, for example “192.168.1.1.”

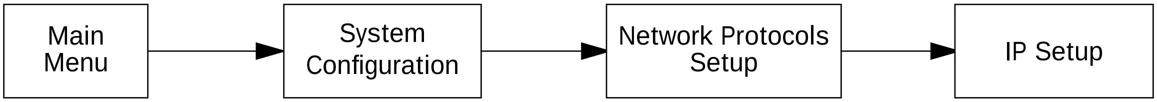
The console screen will open to the **Main Menu**, similar to the screen shown below:



```
                              Netopia R2020 v4.4

                        Easy Setup...

                        WAN Configuration...

                        System Configuration...

                        Utilities & Diagnostics...

                        Statistics & Logs...

                        Quick Menus...

                        Quick View...



Return/Enter goes to Easy Setup -- minimal configuration.
You always start from this main screen.
```

Navigating through the System Configuration screens

To help you find your way to particular screens, some sections in this guide begin with a graphical path guide similar to the following example:



This particular path guide shows how to get to the Network Protocols Setup screens. The path guide represents these steps:

1. Beginning in the Main Menu, select the **System Configuration** item and press Return.
2. Select the **Network Protocols** item in the System Configuration screen and press Return.
3. Select the **IP Setup** item in the Network Protocols Setup screen and press Return.

To go back in this sequence of screens, use the Escape key.

System Configuration features

SmartStart may be all you need to configure your Netopia R2020. Some users, however, require advanced settings or prefer manual control over the default selections that SmartStart automatically chooses. For these users, the Netopia R2020 provides System Configuration options.

To help you determine whether you need to use the System Configuration options, review the following requirements. If you have one or more of these needs, use the System Configuration options described in the later chapters.

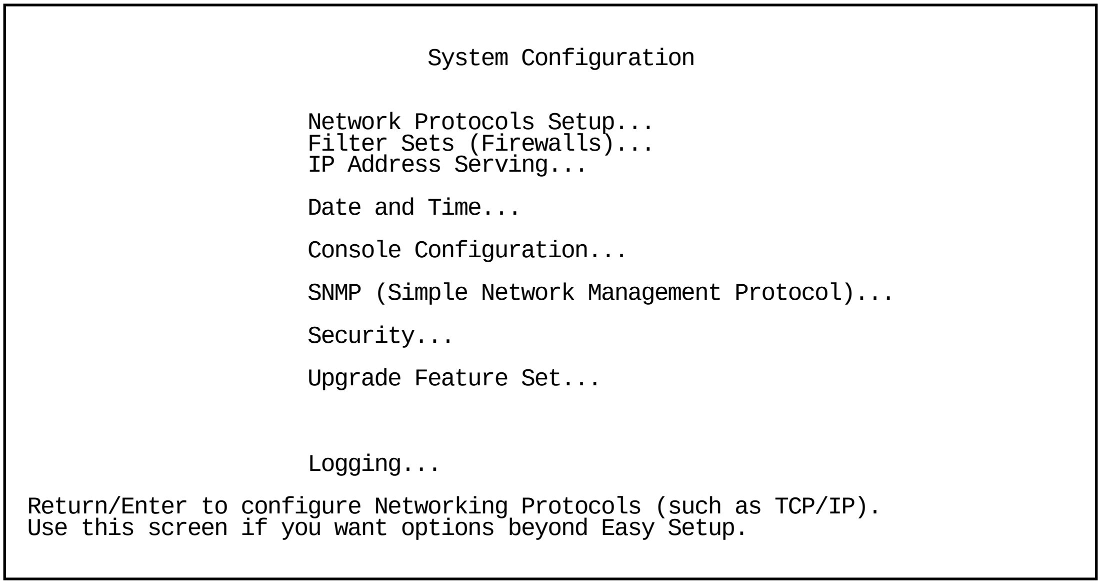
- Two or more outgoing connection profiles to connect to more than one remote location (for example, to connect to the Internet and to a network at another office).
- System Configuration of dynamic IP address distribution through DHCP, MacIP, or BootP.
- Customized incoming call profile to control received calls.
- Scheduled connections.
- Greater network security through the use of filters, CallerID, callback, and SecurID.
- System Configuration of AppleTalk LAN settings.
- System Configuration of connections to AppleTalk networks through the Internet or any IP network, using AURP (AppleTalk “tunneling”).
- System Configuration of connection profiles. See the table below for a partial list of the options available through System Configuration.

Layer Category	Parameter Type	Options	Default settings
Protocol Layer	IP Parameters	Filter Sets:	Basic Firewall NetBIOS Filter
		Receive RIP:	Both
		Transmit RIP:	Off
	IPX Parameters	Path Delay:	1 second
		NetBios Packet Forwarding:	No
		Incoming/outgoing Packet & SAP filter:	On
		Periodic RIP/SAP timers:	60 seconds
Datalink Layer	PPP/MP Parameters	Data Compression:	Standard LZS
		Send Authentication:	PAP
		Channel Usage:	Dynamic
		Bandwidth Allocation:	BAP
		Maximum Packet Size:	1500

Layer Category	Parameter Type	Options	Default settings
Physical Layer	Telco Parameters	Dial is set to:	Dial In/Out
		Dial On Demand is set to:	Yes
		Callback is set to:	No
		Idle Time-out is set for:	300 seconds

To access the System Configuration screens, select **System Configuration** in the Main Menu, then press Return.

The System Configuration Menu screen appears:



```
                           System Configuration

                      Network Protocols Setup...
                      Filter Sets (Firewalls)...
                      IP Address Serving...

                      Date and Time...

                      Console Configuration...

                      SNMP (Simple Network Management Protocol)...

                      Security...

                      Upgrade Feature Set...


                      Logging...

Return/Enter to configure Networking Protocols (such as TCP/IP).
Use this screen if you want options beyond Easy Setup.
```

Network Protocols Setup

These screens allow you to configure your network's use of the standard networking protocols:

- IP: details are given in "Multiple Network Address Translation and IP Setup" on page 10-1.
- IPX: details are given in "IPX Setup" on page 11-1.
- AppleTalk: details are given in "AppleTalk Setup" on page 12-1.

  Note: AppleTalk requires the optional AppleTalk feature expansion kit.

Filter Sets (Firewalls)

These screens allow you to configure security on your network by means of filter sets and a basic firewall.

- Details are given in "Security" on page 14-1.

IP Address Serving

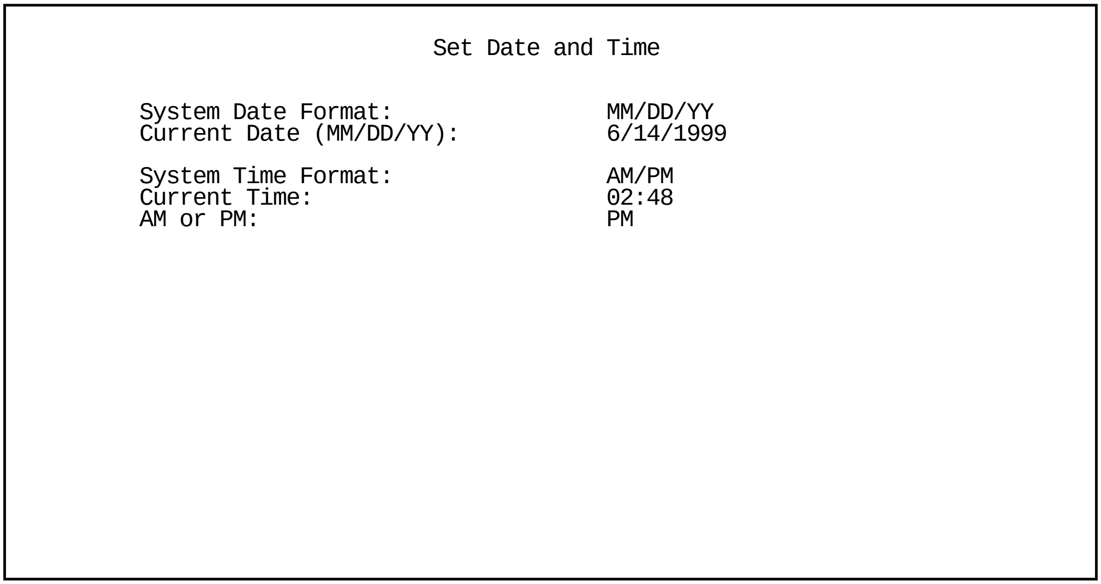
These screens allow you to configure IP Address serving on your network by means of DHCP, WANIP, BootP, and with the optional AppleTalk kit, MacIP.

- Details are given in "IP address serving" on page 10-35.

Date and Time

You can set the system's date and time in the **Set Date and Time** screen.

Select **Date and Time** in the System Configuration screen and press Return to go to the Set Date and Time screen.



```
                         Set Date and Time

         System Date Format:                  MM/DD/YY
         Current Date (MM/DD/YY):             6/14/1999

         System Time Format:                  AM/PM
         Current Time:                        02:48
         AM or PM:                            PM
```

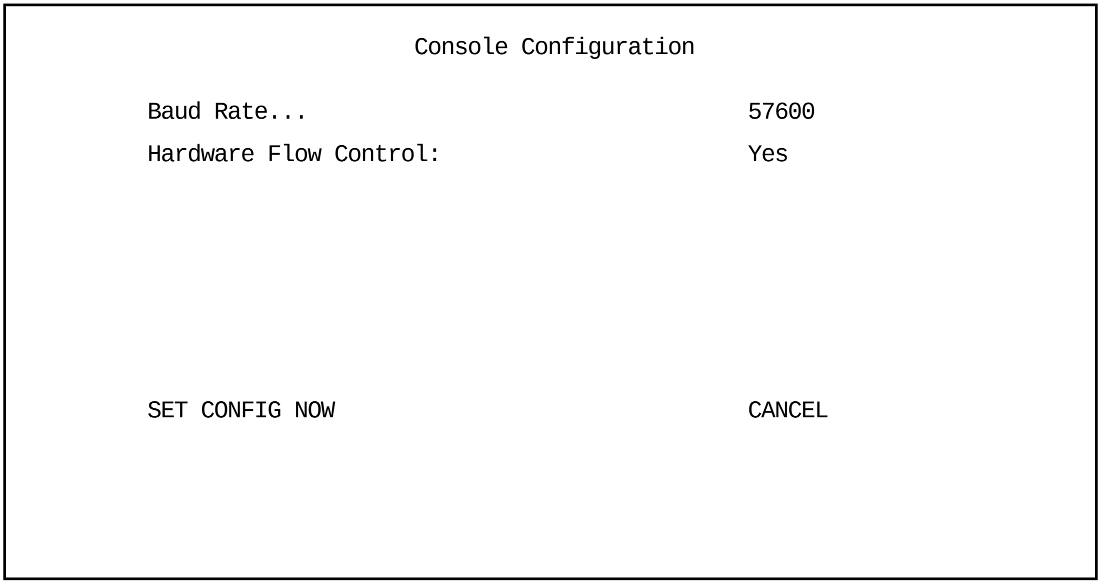
Follow these steps to set the system's date and time:

1. Select **System Date Format** and press Return. A pop-up menu offers you the choice of date format: MM/DD/YY (the default), DD/MM/YY, or YY/MM/DD.
2. Select **Current Date** and enter the date in the appropriate format. Use one- or two-digit numbers for the month and day, and the last two digits of the current year. The date's numbers must be separated by forward slashes (/).
3. Select **Current Time** and enter the time in the format HH:MM, where HH is the hour (using either the 12-hour or 24-hour clock) and MM is the minutes.
4. Select **AM or PM** and choose **AM** or **PM**.

Console Configuration

You can change the default terminal communications parameters to suit your requirements.

To go to the Console Configuration screen, select **Console Configuration** in the System Configuration screen.



```
                              Console Configuration

          Baud Rate...                                  57600
          Hardware Flow Control:                        Yes





          SET CONFIG NOW                                CANCEL
```

Follow these steps to change a parameter's value:

1. Select the parameter you want to change.
2. Select a new value for the parameter. Return to step 1 if you want to configure another parameter.
3. Select **SET CONFIG NOW** to save the new parameter settings. Select **CANCEL** to leave the parameters unchanged and exit the Console Configuration screen.

SNMP (Simple Network Management Protocol)

These screens allow you to monitor and configure your network by means of a standard Simple Network Management Protocol (SNMP) agent.

- Details are given in "SNMP" on page 13-12.

Security

These screens allow you to add users and define passwords on your network.

- Details are given in "Security" on page 14-1.

Upgrade Feature Set

You can upgrade your Netopia R2020 by adding new feature sets through the **Upgrade Feature Set** utility.

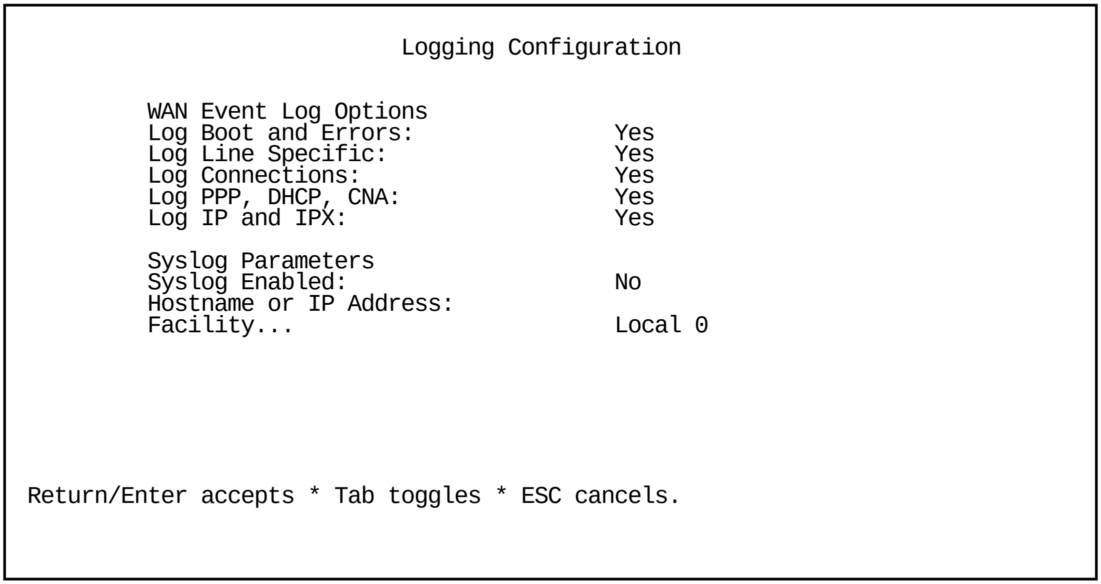
See the release notes that came with your router or feature set upgrade or visit the Netopia web site at www.netopia.com for information on new feature sets, how to obtain them, and how to install them on your Netopia R2020.

Logging

You can configure a UNIX-compatible syslog client to report a number of subsets of the events entered in the router’s WAN Event History. See “WAN Event History” on page 13-6.The Syslog client (for the PC only) is supplied as a .ZIP file on the Netopia CD.

Select **Logging** from the System Configuration menu.

The Logging Configuration screen appears.



```
                            Logging Configuration


         WAN Event Log Options
         Log Boot and Errors:               Yes
         Log Line Specific:                 Yes
         Log Connections:                   Yes
         Log PPP, DHCP, CNA:                Yes
         Log IP and IPX:                    Yes

         Syslog Parameters
         Syslog Enabled:                    No
         Hostname or IP Address:
         Facility...                        Local 0







Return/Enter accepts * Tab toggles * ESC cancels.
```

By default, all events are logged in the event history.

- By toggling each event descriptor either **Yes** or **No**, you can determine which ones are logged and which are ignored.
- You can enable or disable the syslog client dynamically. When enabled, it will report any appropriate and previously unreported events.
- You can specify the syslog server’s address either in dotted decimal format or as a DNS name up to 63 characters.
- You can specify the UNIX syslog Facility to use by selecting the **Facility** pop-up.

Installing the Syslog client

The Goodies folder on the Netopia CD contains a Syslog client daemon program that can be configured to report the WAN events you specified in the Logging Configuration screen.

To install the Syslog client daemon, exit from the graphical Netopia CD program and locate the CD directory structure through your Windows desktop, or through Windows Explorer. Go to the Goodies directory on the CD and locate the Sds15000.exe program. This is the Syslog daemon installer. Run the Sds15000.exe program and follow the on screen instructions for enabling the Windows Syslog daemon.

When using **syslog** with a switched connection, if the host you are logging into is located on the WAN, the act of tearing down the call generates WAN events. This requires the torn down line to come back up, effectively making a call that will go up and down continuously. This will only occur when the router tears down the call. If the call is cleared remotely the redial restriction takes precedence and the packets are transparently aged out of the queue.

The following screen shows a sample syslog dump of WAN events:

```
April 5 10:14:06 tsnext.netopia.com   Link 1 down: PPP PAP failure
April 5 10:14:06 tsnext.netopia.com >>Issued Speech Setup Request from our DN: 5108645534
April 5 10:14:06 tsnext.netopia.com   Requested Disc. from DN: 917143652500
April 5 10:14:06 tsnext.netopia.com   Received Clear Confirm for our DN: 5108645534
April 5 10:14:06 tsnext.netopia.com   Link 1 down: Manual disconnect
April 5 10:14:06 tsnext.netopia.com >>Issued Speech Setup Request from our DN: 5108645534
April 5 10:14:06 tsnext.netopia.com   Requested Disc. from DN: 917143652500
April 5 10:14:06 tsnext.netopia.com   Received Clear Confirm for our DN: 5108645534
April 5 10:14:06 tsnext.netopia.com   Link 1 down: No answer
April          5          10:14:06          tsnext.netopia.com          --Device
restarted---------------------------------------
April 5 10:14:06 tsnext.netopia.com >>WAN: 56K Modem 1 activated at 115 Kbps
April 5 10:14:06 tsnext.netopia.com   Connect Confirmed to our DN: 5108645534
April 5 10:14:06 tsnext.netopia.com   PPP: Channel 1 up, Answer Profile name: Default Profile
April 5 10:14:06 tsnext.netopia.com    PPP: NCP up, session 1, Channel 1 Final (fallback)
negotiated auth: Local PAP , Remote NONE
April 5 10:14:06 tsnext.netopia.com  PPP: PAP  we accepted remote, Channel 1 Remote name: guest
April  5  10:14:06  tsnext.netopia.com    PPP:  MP  negotiated,  session  1  Remote  EDO:  06  03
0000C5700624 0
April 5 10:14:06 tsnext.netopia.com   PPP: CCP negotiated, session 1, type: Ascend LZS Local
mode: 1, Remote mode: 1
April 5 10:14:06 tsnext.netopia.com  PPP: BACP negotiated, session 1 Local MN: FFFFFFFF, Remote
MN: 00000001
April 5 10:14:06 tsnext.netopia.com   PPP: IPCP negotiated, session 1, rem: 192.168.10.100
local: 192.168.1.1
April 5 10:14:06 tsnext.netopia.com >>WAN: 56K Modem 1 deactivated
April 5 10:14:06 tsnext.netopia.com   Received Clear Ind. from DN: 5108645534, Cause: 0
April 5 10:14:06 tsnext.netopia.com   Issued Clear Response to DN: 5108645534
April 5 10:14:06 tsnext.netopia.com   Link 1 down: Remote clearing
April 5 10:14:06 tsnext.netopia.com   PPP: IPCP down, session 1
April 5 10:14:06 tsnext.netopia.com >>Received Speech Setup Ind. from DN: (not supplied)
```

Chapter 8

Managing Data Calls

You can set a Netopia Router to make scheduled connections using designated connection profiles. This is useful for creating and controlling regularly scheduled periods when the router can be used by hosts on your network. It is also useful for once-only connections that you want to schedule in advance.

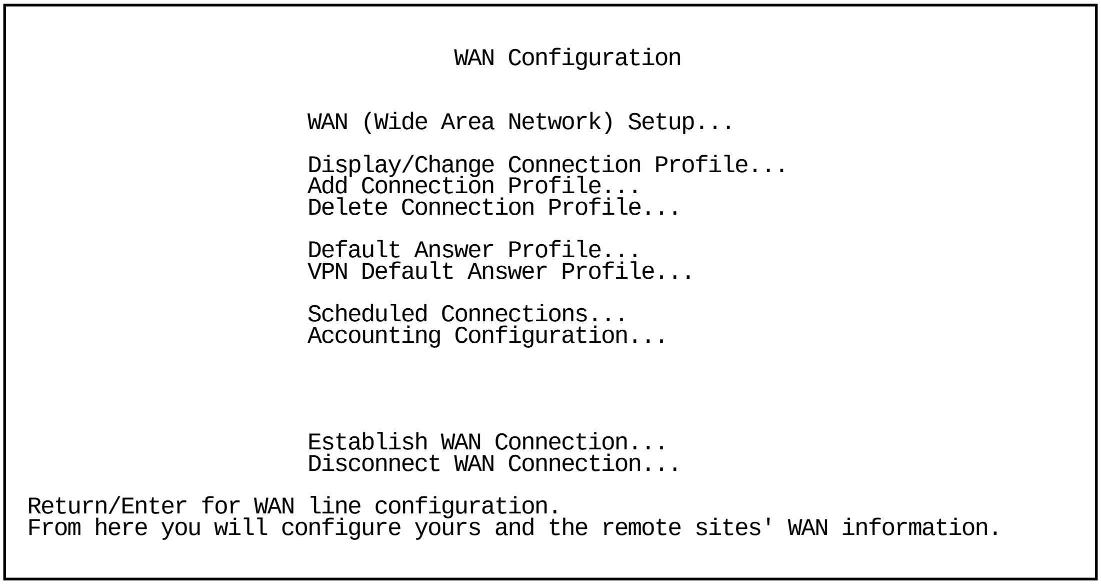
The Netopia R2020 Dual Analog Router can answer calls as well as initiate them. To answer calls, the Netopia R2020 uses a Default Answer Profile. The Default Answer Profile controls how incoming calls are set up, authenticated, filtered, and more.

Topics in this chapter include:

- "Specifying telephone connections" on page 8-1
- "Default Answer Profile for Dial-in Connections" on page 8-4
- "Scheduled connections" on page 8-7
- "Connection Metering" on page 8-12

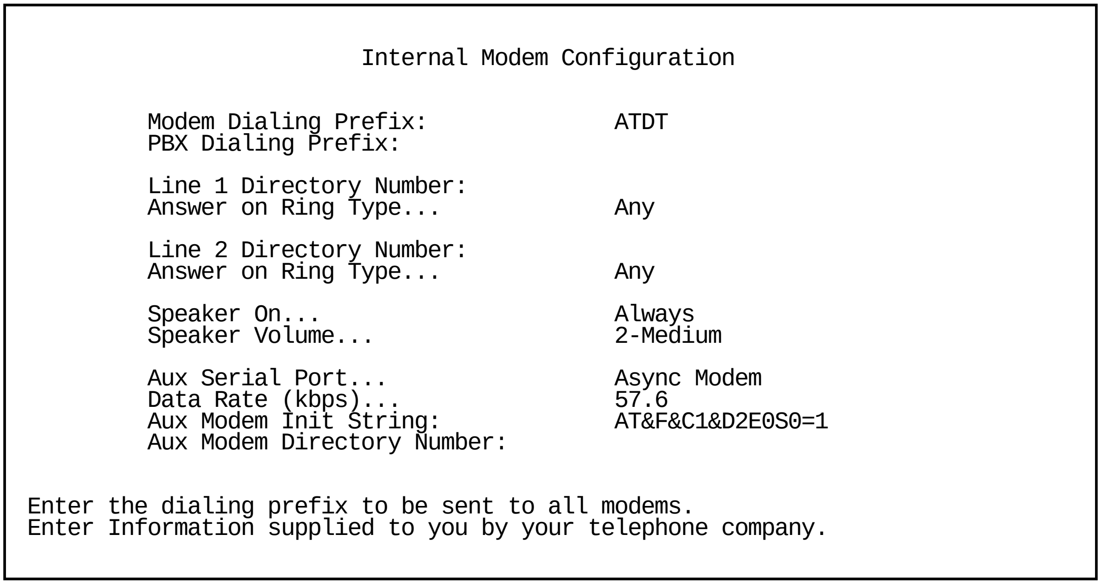
Specifying telephone connections

You can configure telephone connections in the **WAN Configuration** screen under the **Main Menu**. Select **WAN (Wide Area Network) Setup**.



```
                                 WAN Configuration

                      WAN (Wide Area Network) Setup...

                      Display/Change Connection Profile...
                      Add Connection Profile...
                      Delete Connection Profile...

                      Default Answer Profile...
                      VPN Default Answer Profile...

                      Scheduled Connections...
                      Accounting Configuration...



                      Establish WAN Connection...
                      Disconnect WAN Connection...

Return/Enter for WAN line configuration.
From here you will configure yours and the remote sites' WAN information.
```

The **Internal Modem Configuration** screen appears.



```
                         Internal Modem Configuration


         Modem Dialing Prefix:              ATDT
         PBX Dialing Prefix:

         Line 1 Directory Number:
         Answer on Ring Type...             Any

         Line 2 Directory Number:
         Answer on Ring Type...             Any

         Speaker On...                      Always
         Speaker Volume...                  2-Medium

         Aux Serial Port...                 Async Modem
         Data Rate (kbps)...                57.6
         Aux Modem Init String:             AT&F&C1&D2E0S0=1
         Aux Modem Directory Number:


Enter the dialing prefix to be sent to all modems.
Enter Information supplied to you by your telephone company.
```

- You can enter a PBX or Centrex Dialing Prefix such as "9" if you are on a PBX or Centrex phone system and require a prefix for an outside line.

- Enter the optional telephone or **Directory Numbers** for the two onboard modems to provide the Netopia R2020 with the information needed to establish a two-channel call using MP or BAP. This will advise the remote side of an inbound data call how to connect to a second channel.

  Note: When placing multi-channel calls, the answering equipment must either:

  - be in a "hunt group," where a single telephone number services multiple lines, or

  - the answering side must implement MP or BAP as a method to advise the calling side what number(s) to use.

    ISPs or corporate IS groups will meet these conditions. For other non-standard dialup connections, you should verify that one or the other of these conditions is true.

- You may choose to selectively **Answer** inbound calls, based on a distinctive ring pattern, on each onboard modem. This permits you to set up a party line configuration where a fax machine or other device shares the line, but uses a different telephone number and ring pattern. Supported options are:

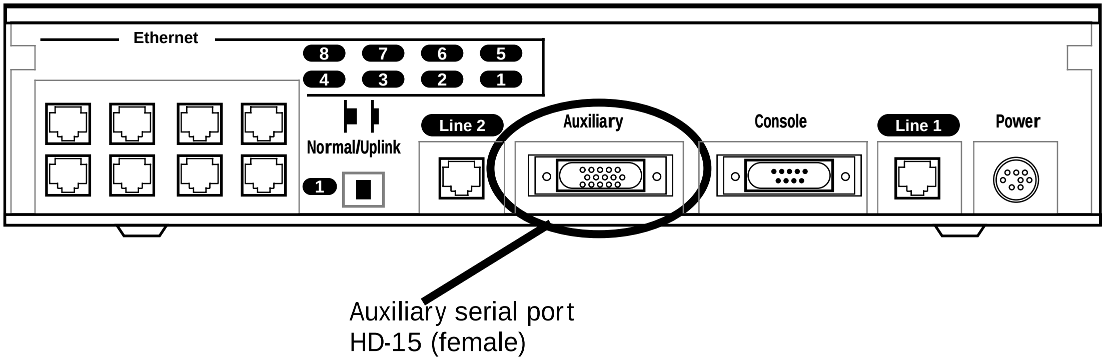
Ring Type:	Description:
Any	(the default) any pattern
Ring A	2.0 sec ON, 4.0 sec OFF (normal North American ring pattern)
Ring B	0.8 sec ON, 0.4 sec OFF, 0.8 sec ON, 4.0 sec OFF
Ring C	0.4 sec ON, 0.2 sec OFF, 0.4 sec ON, 0.2 sec OFF, 0.8 sec ON, 4.0 sec OFF
Never	the line will not answer to any ring pattern

- You can choose when the Netopia R2020’s modem connection tones are audible. Supported options are:

Selection:	Behavior:
Never	Turns off all speaker activity and hides the **Speaker Volume** control.
Until Carrier	The default. Allows call placement and handshaking tones to be heard.
During Answer	Same as above, but blocks dialing tones.
Always	Allows carrier tones to be heard, as well.

- You can specify how to use the auxiliary serial port on the Netopia R2020’s back panel. By default, this port is enabled for an external asynchronous modem. If you have installed the optional AppleTalk feature set, then this port defaults to a LocalTalk connection. See “AppleTalk Setup” on page 12-1 for more information on how to use the optional AppleTalk feature set.

Netopia R2020 back panel



For external modem applications, the **Data Rate** pop-up offers a variety of clock rates from 9600 to 230 Kbps. The default is 57.6 kbps.

You can also specify the **Modem Init String** for your modem and the **Directory Number** of the telephone line connected to the third port.

Note: If you change the modem init string, you must restart the system. From the Main Menu, go to Utilities & Diagnostics and select Restart System. The router will reboot, and your changes will be in effect.

Default Answer Profile for Dial-in Connections

The Netopia R2020 Dual Analog Router can answer calls as well as initiate them. To answer calls, the Netopia R2020 uses a Default Answer Profile. The Default Answer Profile controls how incoming calls are set up, authenticated, filtered, and more.

How the Default Answer Profile works

The Default Answer Profile works like a guard booth at the gate to your network: it scrutinizes incoming calls. Like the guard booth, the Default Answer Profile allows calls based on a set of criteria that you define.

The main criterion used to check calls is whether they match one of the Connection Profiles already defined. If PAP or CHAP authentication is being used, the default profile checks that the incoming call's name and password/secret match the receive name and password/secret of a Connection Profile. If PAP or CHAP is not being used, an incoming call is matched to a Connection Profile using the remote network's IP address (that is, the caller is defined as the destination of a particular connection profile).

If an incoming call is matched to an existing Connection Profile, the call is accepted. All of that Connection Profile's parameters, except for authentication, are adopted for the call.

You could set up the Default Answer Profile to allow calls in even if they fail to match a Connection Profile. Continuing the guard booth analogy, this would be like removing the guards or having them wave all calls in, regardless of their source.

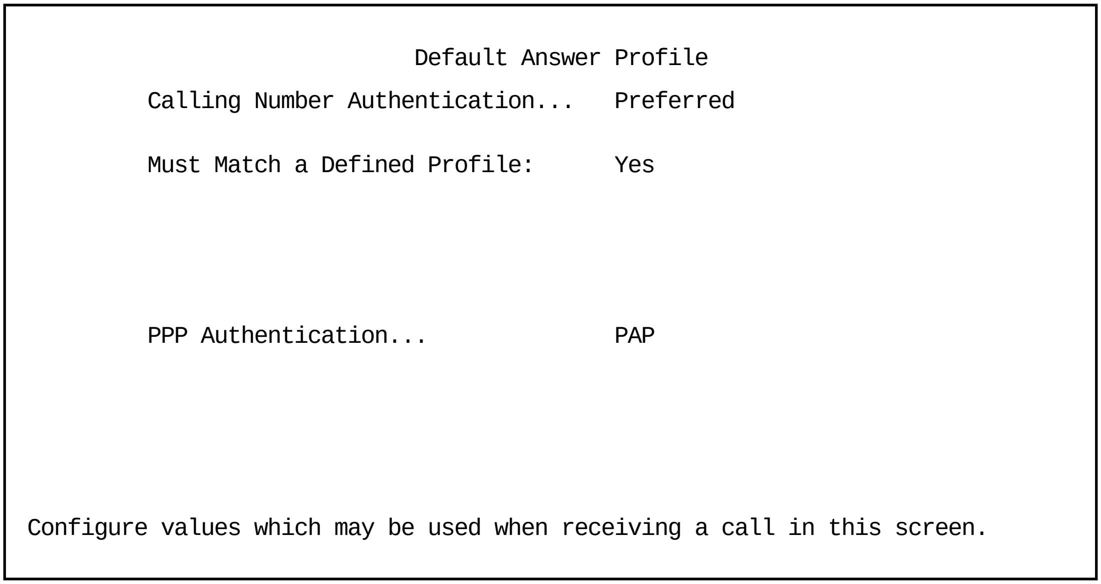
If an incoming call is not required to match a connection profile, and fails to do so, it is accepted as a standard IP connection. Accepted, unmatched calls adopt the call parameter values set in the Default Answer Profile.

To determine the call parameter values that unmatched calls will adopt, customize the Default Answer Profile parameters in the Default Answer Profile screen.

Customizing the default profile

You can customize the Netopia Router's default profile in the Default Answer Profile screen.

1. Select **Default Answer Profile** in the WAN Configuration screen. Press Return. The Default Profile screen appears.



```
                            Default Answer Profile
            Calling Number Authentication...   Preferred

            Must Match a Defined Profile:      Yes




            PPP Authentication...              PAP





Configure values which may be used when receiving a call in this screen.
```

2. To enable CNA-authentication, select **Calling Number Authentication** in the Default Answer Profile screen and choose one of the following settings:

   Ignored: Calling Number Authentication (CNA) is not in effect.

   Preferred: This is the default setting. Authentication is attempted if the calling number is available. If authentication fails, or the calling number is not available, the call proceeds as usual and the caller may still connect successfully. Use this setting if you expect to receive both regular and CNA-authenticated calls.

   Required: Authentication is attempted if the calling number is available. If authentication fails, or the calling number is not available, the Netopia Router disconnects the caller. Use this setting if you require all calls to be CNA-authenticated.

   Calling Number Authentication (CNA), is an application of CallerID. It is a method of verifying that an incoming call is originating from an expected site. Using CNA, you can increase the security of your network by requiring that callers not only possess the correct PPP authentication information, but also are calling from a particular physical location.

   CNA works by checking the calling number that the Netopia Router receives during the initial setup phase of an incoming call against a set of stored numbers. Each number in the stored set is defined in a specific connection profile. When a match occurs, the incoming call is handled by the connection profile containing the matched number.

   Using CNA can also provide cost savings because calls are not billed during the CNA phase. With CNA, a caller can set up a connection to the Netopia Router without incurring any charges by accessing a dial-back connection profile. If the caller's rates are higher than those charged to the Netopia Router's return call, then using CNA has saved the difference.

CNA should be available where CallerID services are available. You will need to consult with your telephone service provider to find out if your line is provisioned for CallerID.

Also note that if the calling side has instructed the phone company to block delivery of its caller ID, the answering side will not be able to authenticate.

If your line does not support the appropriate service, CNA may not work properly.

3. To force incoming calls to match connection profiles, select **Must Match a Defined Profile** and toggle it to **Yes**. Incoming calls that cannot be matched to a connection profile are dropped. To allow unmatched calls to be accepted as standard IP or IPX connections, toggle **Must Match a Defined Profile** to **No**.

   If **Must Match a Defined Profile** is set to **Yes**, the answer profile only accepts calls that use the same authentication method defined in the **Authentication** item. If PAP or CHAP are involved, the caller must have a name and password or secret that match one of the connection profiles. The caller must obtain these from you or your network administrator before initiating the call.

   For example, if **Must Match a Defined Profile** is set to **Yes**, and **Authentication** is set to **PAP**, then only incoming calls that use PAP and match a connection profile will be accepted by the answer profile.

   If authentication in the Default Answer Profile is set to CHAP, the value of the **CHAP Challenge Name** item must be identical to the value of the **Send Host Name** item of the Connection Profile to be matched by the caller.

   If **Must Match a Defined Profile** is set to **No**, **Authentication** is assumed to be **None**, even if you’ve set it to **PAP** or **CHAP.** The answer profile uses the caller’s IP address to match a connection profile. However, the answer profile cannot discover a caller’s subnet mask; it assumes that the caller is *not* subnetting its IP address:

   Class A addresses are assumed to have a mask of 255.0.0.0

   Class B addresses are assumed to have a mask of 255.255.0.0

   Class C addresses are assumed to have a mask of 255.255.255.0. Class C address ranges are generally the most common subnet allocated.

   If a remote network has a non-standard mask (that is, it uses subnetting), the only way for it to successfully connect to the Netopia Router is by matching a connection profile. In other words, you will have to set up a connection profile for that network.If **Must Match a Defined Profile** is set to **No**, you can also set the following parameters for accepted calls that do not match a connection profile:

Call acceptance scenarios

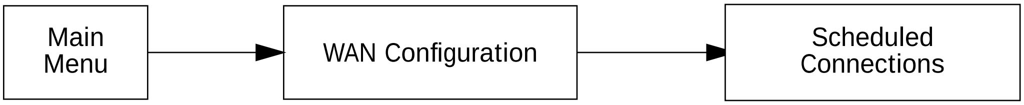
The following are a few common call acceptance scenarios and information on how to configure the Netopia R2020 for those purposes.

- To accept all calls, regardless of whether they match a connection profile:
  - Toggle **Must Match a Defined Profile** to **No**.
- To only accept calls that match a connection profile through use of a name and password (or secret):
  - Toggle **Must Match a Defined Profile** to **Yes**, *and*
  - Set **Authentication** to **PAP** or **CHAP**.

Note: The authentication method you choose determines which connection profiles are accessible to callers. For example, if you choose PAP, callers using CHAP or no authentication will be dropped by the answer profile.

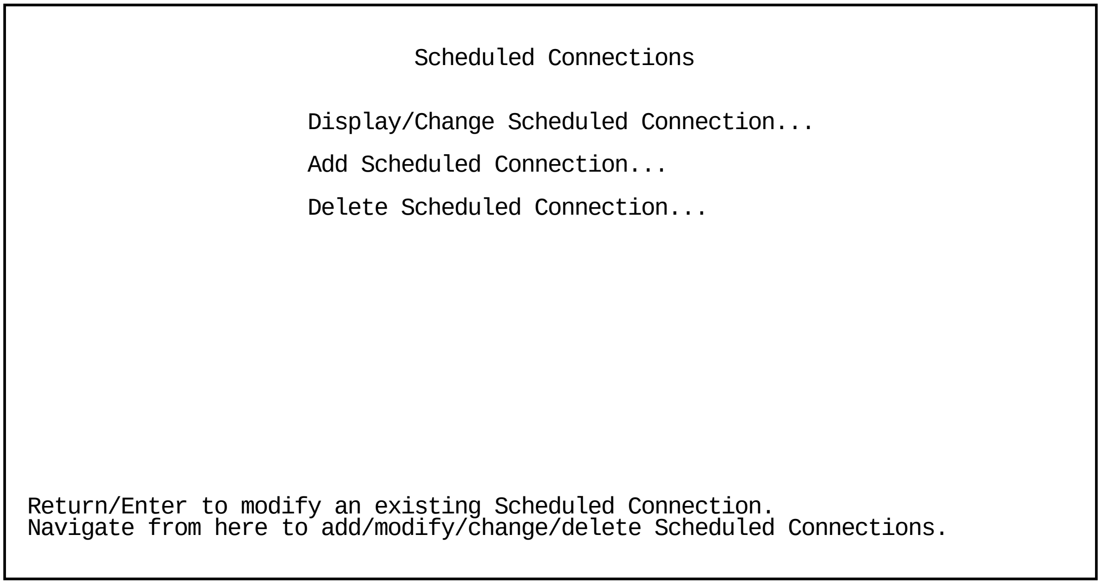
- To allow calls that *only* match a connection profile's remote IP and/or IPX address:
  - Toggle **Must Match a Defined Profile** to **Yes**, *and*
  - set **Authentication** to **None**.
- To not allow *any* incoming calls to connect to the Netopia Router:
  - Toggle **Must Match a Defined Profile** to **Yes**, *and*
  - Set the **Dial** option in the Telco Options screen of every connection profile to **Dial Out Only**

Scheduled connections



You can set a Netopia Router to make scheduled connections using designated connection profiles. This is useful for creating and controlling regularly scheduled periods when the router can be used by hosts on your network. It is also useful for once-only connections that you want to schedule in advance.

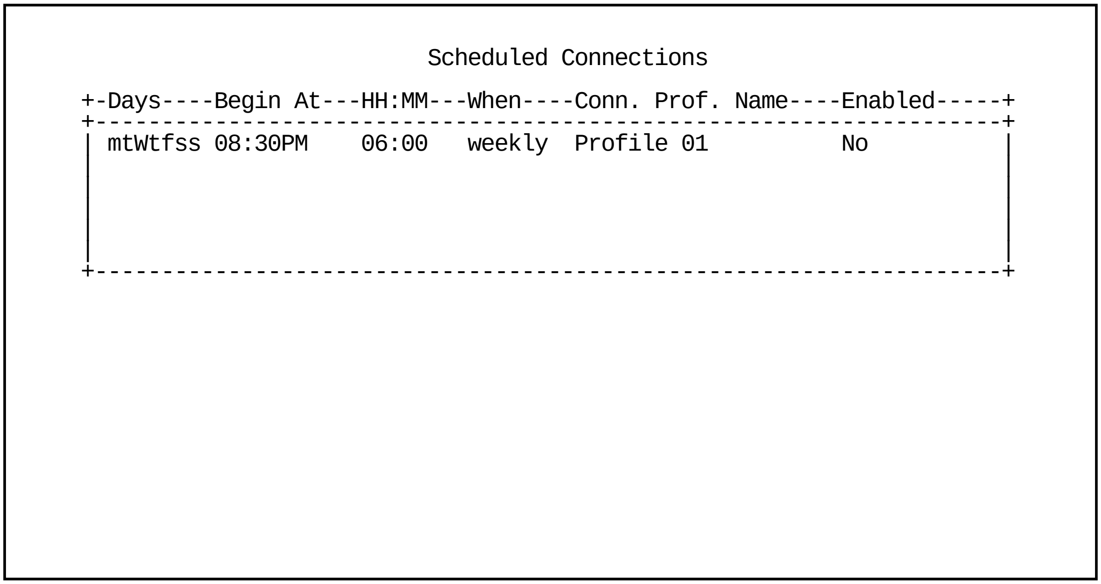
To go to the Scheduled Connections screen, select **Scheduled Connections** in the WAN Configuration screen.



```
                         Scheduled Connections

                    Display/Change Scheduled Connection...

                    Add Scheduled Connection...

                    Delete Scheduled Connection...










Return/Enter to modify an existing Scheduled Connection.
Navigate from here to add/modify/change/delete Scheduled Connections.
```

Viewing scheduled connections

To display a table of view-only scheduled connections, select **Display / Change Scheduled Connection** in the Scheduled Connections screen. Each scheduled connection occupies one row of the table.



```
                          Scheduled Connections

+-Days----Begin At---HH:MM---When----Conn. Prof. Name-----Enabled-----+
+---------------------------------------------------------------------+
| mtWtfss 08:30PM    06:00   weekly  Profile 01          No           |
|                                                                     |
|                                                                     |
|                                                                     |
|                                                                     |
+---------------------------------------------------------------------+
```

The first column in the table shows a one-letter representation of the **Days** of the week, from Monday (M or m) to Sunday (S or s). If a letter representing a day is capitalized, the connection will be activated on that day; a lower-case letter means that the connection will not be activated on that day. If the scheduled connection is configured for a once-only connection, the word “once” will appear instead of the days of the week.

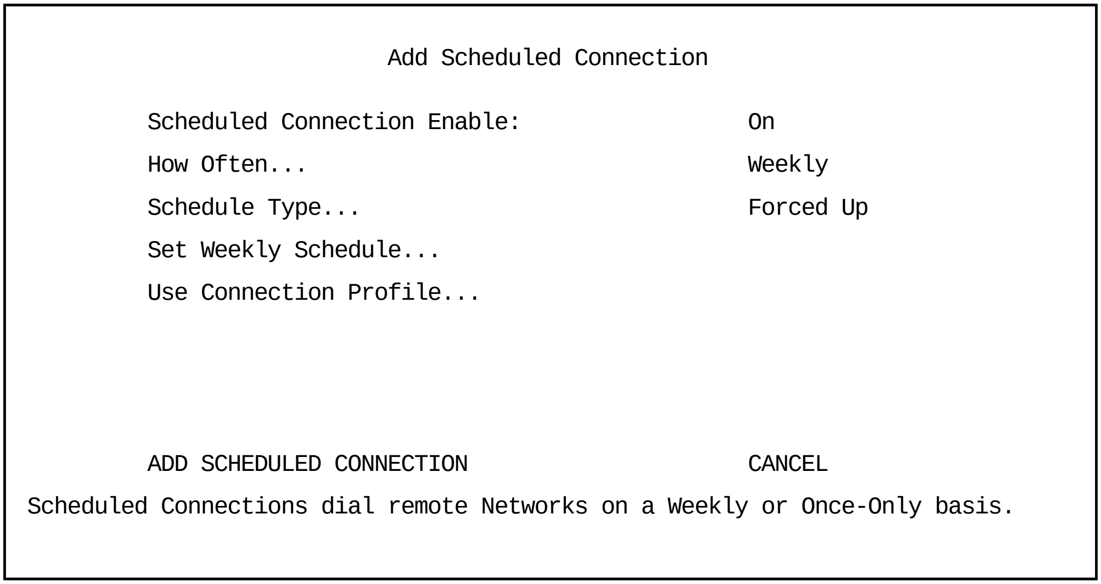
The other columns show:

- The time of day that the connection will **Begin At**
- The duration of the connection (**HH:MM**)
- Whether it's a recurring **Weekly** connection or used **Once Only**
- Which connection profile (**Conn. Prof.**) is used to connect
- Whether the scheduled connection is currently **Enabled**

The router checks the date and time set in scheduled connections against the system date and time.

Adding a scheduled connection

To add a new scheduled connection, select **Add Scheduled Connection** in the Scheduled Connections screen and press Return. The Add Scheduled Connection screen appears.



```
                      Add Scheduled Connection

         Scheduled Connection Enable:                On
         How Often...                                Weekly
         Schedule Type...                            Forced Up
         Set Weekly Schedule...
         Use Connection Profile...




         ADD SCHEDULED CONNECTION                    CANCEL
Scheduled Connections dial remote Networks on a Weekly or Once-Only basis.
```

Follow these steps to configure the new scheduled connection:

- To activate the connection, select **Scheduled Connection Enable** and toggle it to **On**. You can make the scheduled connection inactive by toggling **Scheduled Connection Enable** to **Off**.
- Decide how often the connection should take place by selecting **How Often** and choosing **Weekly** or **Once Only** from the pop-up menu.
- The **Schedule Type** item directly below **How Often** allows you to set the type of schedule. Options are:.

Selection:	Behavior:
Forced Up	(the default) establishes and maintains the connection for the schedule period specified
Forced Down	tears down and prevents any connection for the schedule period specified
Demand-Allowed	permits demand calls for the schedule period specified
Demand-Blocked	blocks demand calls for the schedule period specified
Periodic	establishes and maintains the connection for a specified period for the duration of the scheduled connection

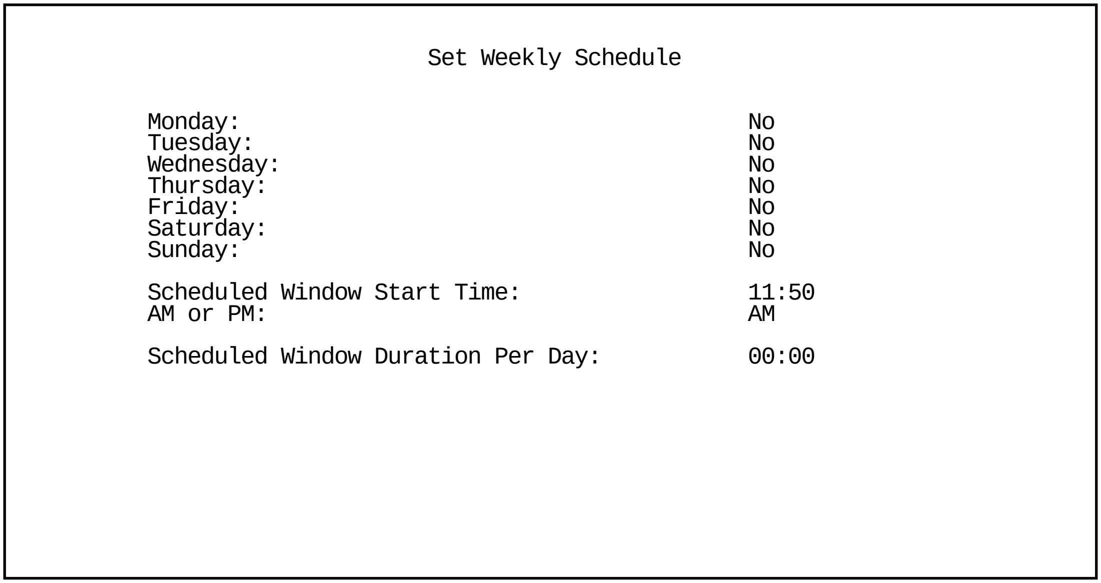
- If **How Often** is set to **Weekly**, the item directly below Schedule Type reads **Set Weekly Schedule**. If **How**

Often is set to **Once Only**, the item directly below **How Often** reads **Set Once-Only Schedule**.

Set Weekly Schedule

If you set **How Often** to **Weekly**, select **Set Weekly Schedule** and go to the Set Weekly Schedule screen.

- Select the days for the scheduled connection to occur and toggle them to **Yes**.



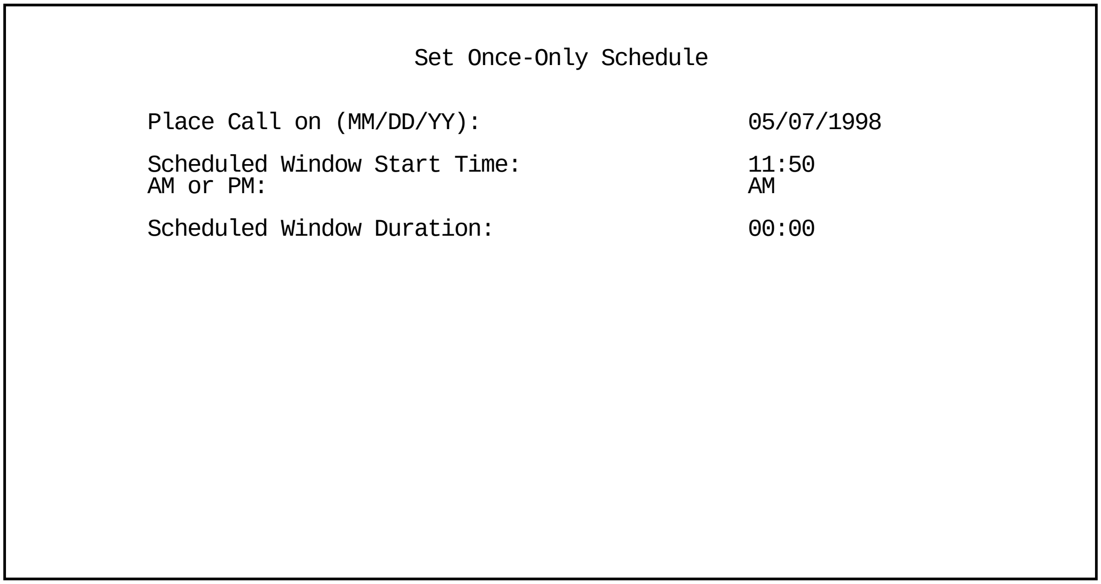
```
                         Set Weekly Schedule

          Monday:                                      No
          Tuesday:                                     No
          Wednesday:                                   No
          Thursday:                                    No
          Friday:                                      No
          Saturday:                                    No
          Sunday:                                      No

          Scheduled Window Start Time:                 11:50
          AM or PM:                                    AM

          Scheduled Window Duration Per Day:           00:00
```

- Select **Scheduled Window Start Time** and enter the time to initiate the scheduled connection.
- You must enter the time in the format H:M, where H is a one- or two-digit number representing the hour and M is a one- or two-digit number representing the minutes. The colon is mandatory. For example, the entry 1:3 (or 1:03) would be accepted as 3 minutes after one o'clock. The entry 7:0 (or 7:00) would be accepted as seven o'clock, exactly. The entries 44, :5, and 2: would be rejected.
- Select **AM or PM** and choose **AM** or **PM** from the pop-up menu.
- Select **Scheduled Window Duration Per Day** and enter the maximum duration allowed for this scheduled connection, per call.
- If you selected Periodic as your Schedule Type in the previous screen, an additional item "Every..." appears. Set the period of time between connections, for example every 15 minutes.

You are finished configuring the weekly options. Return to the Add Scheduled Connection screen to continue.

Set Once-Only Schedule

If you set **How Often** to **Once Only**, select **Set Once-Only Schedule** and go to the Set Once-Only Schedule screen.



```
                       Set Once-Only Schedule

     Place Call on (MM/DD/YY):                    05/07/1998

     Scheduled Window Start Time:                 11:50
     AM or PM:                                    AM

     Scheduled Window Duration:                   00:00
```

- Select **Place Call On (Date)** and enter a date in the format MM/DD/YY or MM/DD/YYYY (month, day, year).

  Note: You must enter the date in the format specified. The slashes are mandatory. For example, the entry 5/7/98 would be accepted as May 7, 1998. The entry 5/7 would be rejected.

- Select **Scheduled Window Start Time** and enter the time to initiate the scheduled connection.

  Note: You must enter the time in the format H:M, where H is a one- or two-digit number representing the hour and M is a one- or two-digit number representing the minutes. The colon is mandatory. For example, the entry 1:3 (or 1:03) would be accepted as 3 minutes after one o'clock. The entry 7:0 (or 7:00) would be accepted as seven o'clock, exactly. The entries 44, :5, and 2: would be rejected.

- Select **AM or PM** and choose **AM** or **PM**.
- Select **Scheduled Window Duration** and enter the maximum duration allowed for this scheduled connection. Use the same format restrictions noted above.

You are finished configuring the once-only options. Return to the Add Scheduled Connection screen to continue.

- In the Add Scheduled Connection screen, select **Use Connection Profile** and choose from the list of connection profiles you have already created. A scheduled connection must be associated with a connection profile to be useful. The connection profile becomes active during the times specified in the associated scheduled connection, if any exists.
- Select **ADD SCHEDULED CONNECTION** to save the current scheduled connection. Select **CANCEL** to exit the Add Scheduled Connection screen without saving the new scheduled connection.

Modifying a scheduled connection

To modify a scheduled connection, select **Change Scheduled Connection** in the Scheduled Connections screen to display a table of scheduled connections.

Select a scheduled connection from the table and go to the Change Scheduled Connection screen. The parameters in this screen are the same as the ones in the Add Scheduled Connection screen (except that **ADD SCHEDULED CONNECTION** and **CANCEL** do not appear). To find out how to set them, see "Adding a scheduled connection" on page 8-8.

Deleting a scheduled connection

To delete a scheduled connection, select **Delete Scheduled Connection** in the Scheduled Connections screen to display a table of scheduled connections.

Select a scheduled connection from the table and press the Return key to delete it. To exit the table without deleting the selected scheduled connection, press the Escape key.

Connection Metering

The Netopia R2020 offers system-wide and per-Connection Profile enhanced connection metering and budgeting. You use this feature to track first minutes (an ISDN tariff factor) and additional minutes or megabytes per time period for initiated data and voice calls, either through the Web-based management pages or the console-based management screens.

Web-based management pages

The Web-based management pages replace the SmartView monitoring tool and add significant new features for managing your router.

You access the Web-based management pages by launching your Web browser and entering the URL:

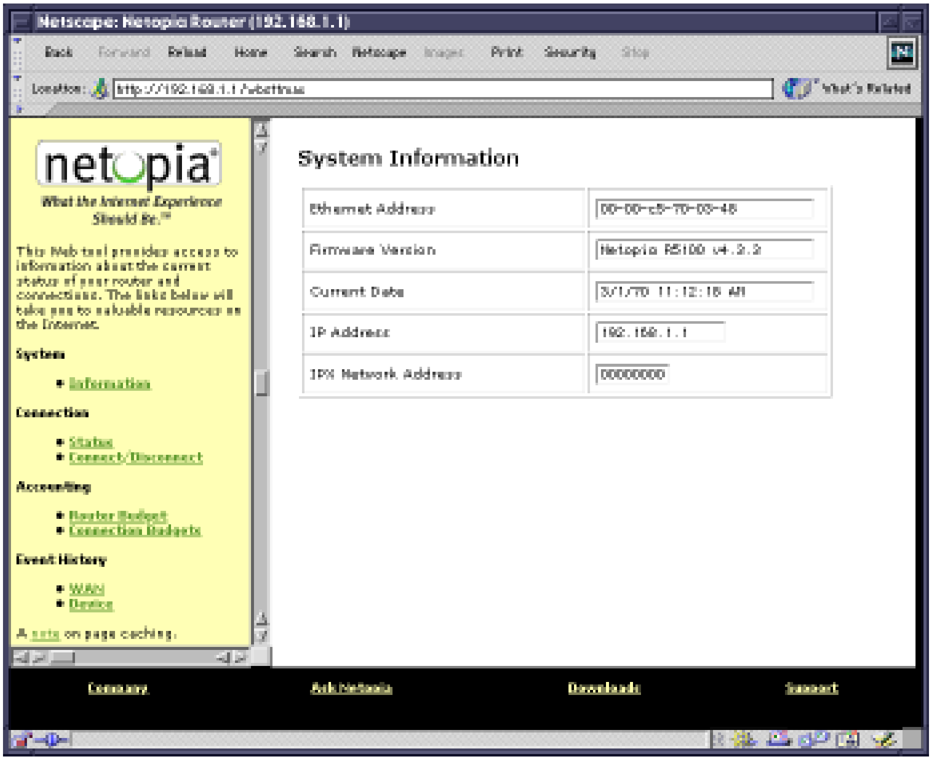
http://*router_IP_address*

where *router_IP_address* is the address of your router. The default address is 198.162.1.1.

The System Information page appears.

System Information page

This is the initial page you link to when you connect to the Web-based management pages.



Netscope: Netopia Router (192.168.1.1)
Back
Forward
Reload
Home
Search
Netscape
Images
Print
Security
Stop
Location: http://192.168.1.1/sbettrue
What's Related
netopia
What the Internet Experience Should Be.™
Company
Ask Netopia
Downloads
Support

This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.

System

- Information

Connection

- Status
- Connect/Disconnect

Accounting

- Router Budget
- Connection Budgets

Event History

- WAN
- Device

A note on page caching.

System Information

Ethernet Address	00-00-c5-70-03-48
Firmware Version	Netopia R5100 v4.2.2
Current Date	3/1/70 11:12:18 AM
IP Address	192.168.1.1
IPX Network Address	00000000

It displays useful general information about your router:

Ethernet Address. The router’s hardware or MAC address

Firmware Version. The router’s model number and current firmware revision level

Current Date. The current date and time, as you have configured them

IP Address. The router’s internal IP address

IPX Network Address. The router’s IPX network address, if you have it enabled and are on an IPX network

The display contains two frames, a navigation frame on the left and the information and configuration page on the right.

The left frame permits you to navigate to:

- System
    - Information screen displays the router’s hardware (MAC) address, the model number and firmware version currently installed, the current date and time, the router’s IP address, and the IPX address, if any.
- Connection
    - “Connection Status page” on page 8-15 *(for frame relay configured devices only)*: displays a snapshot

of the activity for your Frame relay DLCIs.

  - "Connection Status page" on page 8-15 *(for switched interfaces only)*: displays the current state of your switched connection.
  - "Connect/Disconnect page" on page 8-16 *(for switched interfaces only)*: displays a list of your Connection Profiles, allowing you to initiate connections using any one of them.

- Accounting *(for switched interfaces only)*

  If you have a leased line with an unswitched interface, these options do not appear.

  - "Router Budget Configuration page" on page 8-17: allows you to display and edit your aggregate connection accounting statistics and limits.
  - "Connection Budgets page" on page 8-18: allows you to set up and track three connection budgets for cost control purposes.

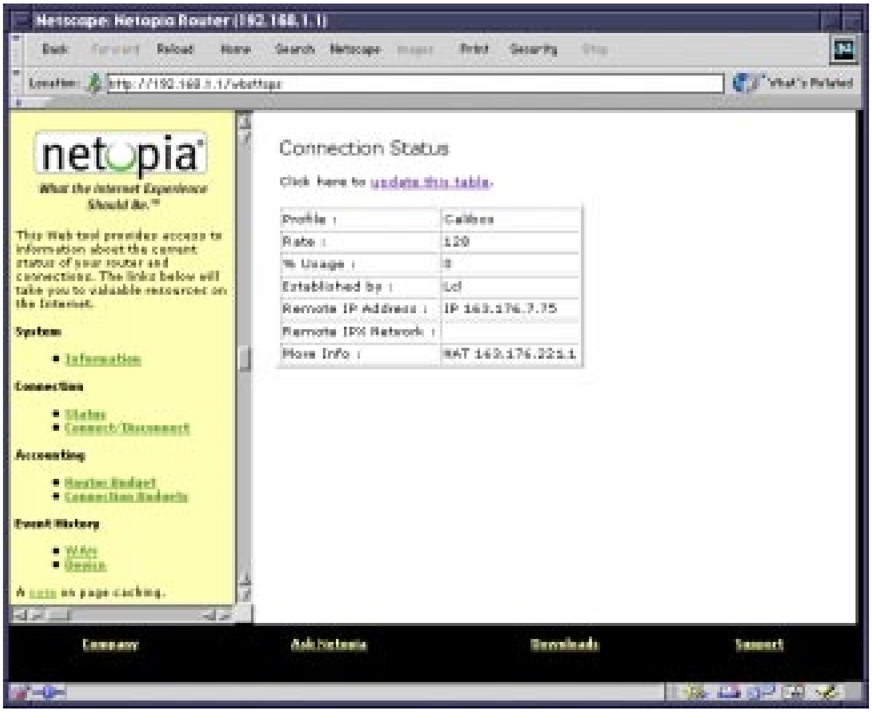
- Event History

  - "WAN Event History page" on page 8-21: displays the most recent events that the router reports for your WAN connections.
  - "Device Event History page" on page 8-22: displays the most recent events that the router reports of its own internal activity.

If you click any link in the left frame, that page is displayed in the right frame.

Connection Status page

For switched interface connections, the Connection Status page displays information for your active Connection Profile and, if applicable, any POTS calls currently active.



Netscape: Netopia Router (192.168.1.1)
Back
Forward
Reload
Home
Search
Netscape
Images
Print
Security
Stop
Location: http://192.168.1.1/wbsttsgs
What's Related
netopia
What the Internet Experience Should Be.™
This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.
System
Information
Connection
Status
Connect/Disconnect
Accounting
Router Budget
Connection Budgets
Event History
WAN
Device
A note on page caching.
Company
Ask Netopia
Downloads
Support

Connection Status

Click here to update this table.

Profile :	Calbox
Rate :	128
% Usage :	0
Established by :	Lcl
Remote IP Address :	IP 163.176.7.75
Remote IPX Network :	
More Info :	NAT 163.176.221.1

The table gives the following information:

Profile. The name you have assigned to the Connection Profile that is currently connected.

Rate. The data rate of this connection.

% Usage. The average percent use of the maximum capacity of the channels in use for the connection.

Established by. Whether the connection was locally (“Lcl”) or remotely (“Rmt”) established.

Remote IP Address. The address of the connection on the remote end.

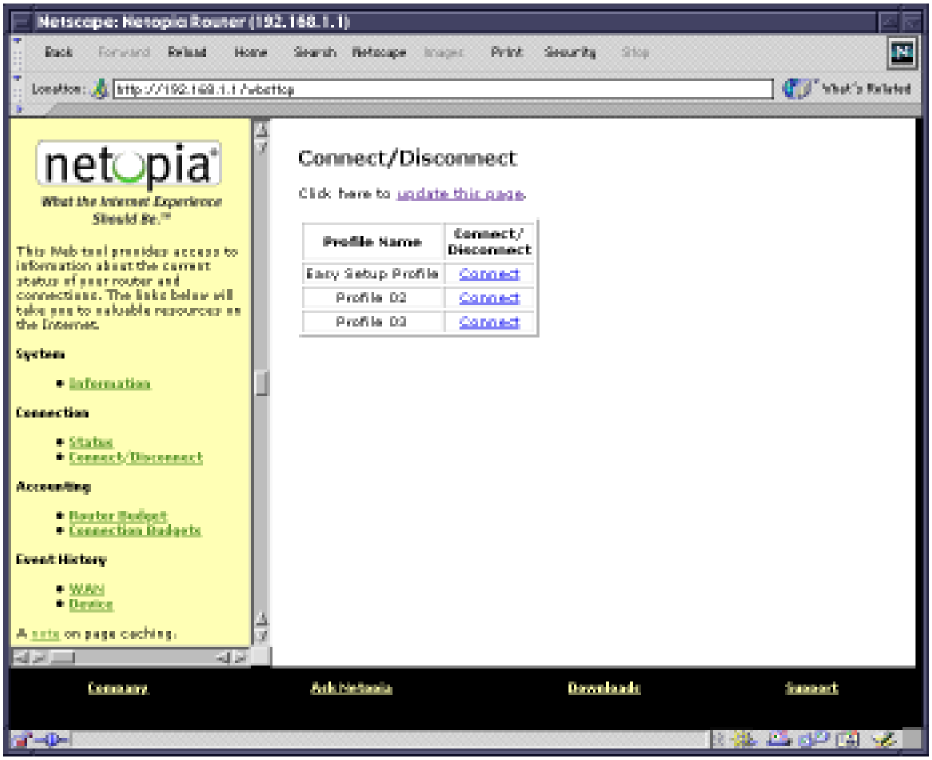
Remote IPX Network. If you are routing IPX traffic, the address of the remote IPX source.

More Info: In order of priority, the NAT address in use for this connection, the IPX address in use (if IP is also in use), or the ISDN caller identification (if available).

To update the information displayed, click the **update this table** link.

Connect/Disconnect page

The Connect/Disconnect page displays a list of your configured Connection Profiles and allows you to connect or disconnect any of them.



Netscape: Netopia Router (192.168.1.1)
Back
Forward
Reload
Home
Search
Netscape
Images
Print
Security
Stop
Location: http://192.168.1.1/webtop
What's Related
netopia
What the Internet Experience Should Be.™
Company
Ask Netopia
Downloads
Support

This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.

System

- Information

Connection

- Status
- Connect/Disconnect

Accounting

- Router Budget
- Connection Budgets

Event History

- WAN
- Device

A note on page caching.

Connect/Disconnect

Click here to update this page.

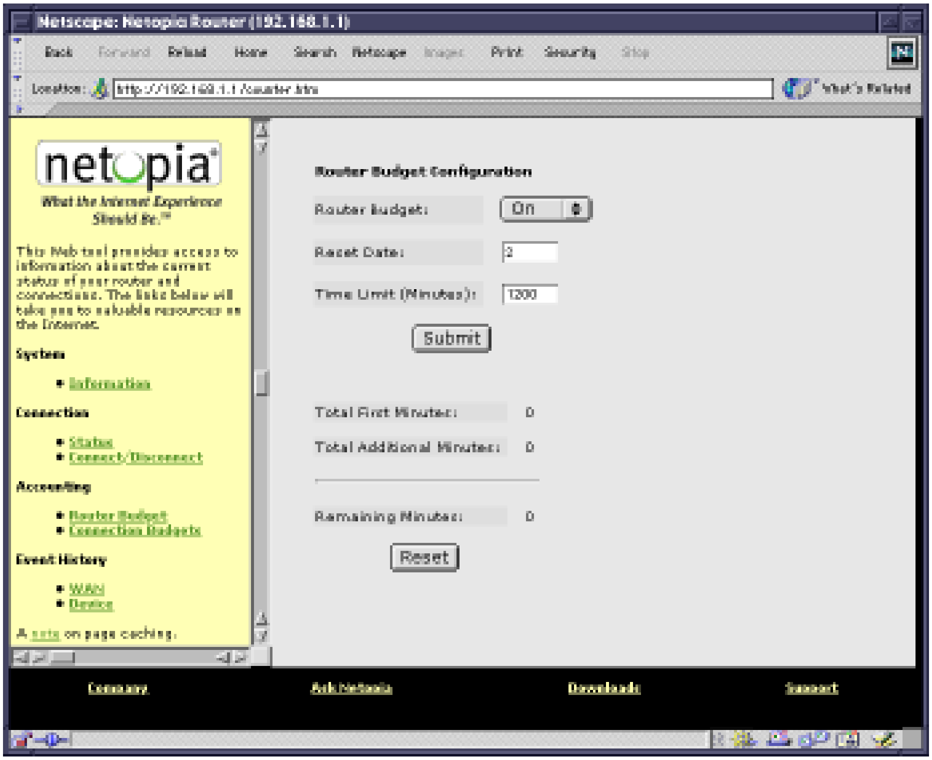
Profile Name	Connect/ Disconnect
Easy Setup Profile	Connect
Profile 02	Connect
Profile 03	Connect

To initiate a connection using any of the displayed Connection Profiles, simply click the **Connect** link.

To disconnect from an active Connection Profile, click the **Disconnect** link.

Router Budget Configuration page

The Router Budget Configuration page allows you to modify the parameters for your overall connection accounting policy.



This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.

A note on page caching.

Router Budget Configuration

Router Budget: On

Reset Date: 2

Time Limit (Minutes): 1200

Total First Minutes: 0

Total Additional Minutes: 0

Remaining Minutes: 0

From this page you can:

- turn **Router Budget** either **On** or **Off** from the pull-down menu
- change the **Reset Date** (day) on which the counters begin counting again
- change the total aggregate **Time Limit** in minutes covered by all of your budgets

If you make any changes in this screen, click the **Submit** button.

To reset the aggregate minute counters to zero again, click the **Reset** button.

The table displays the following information:

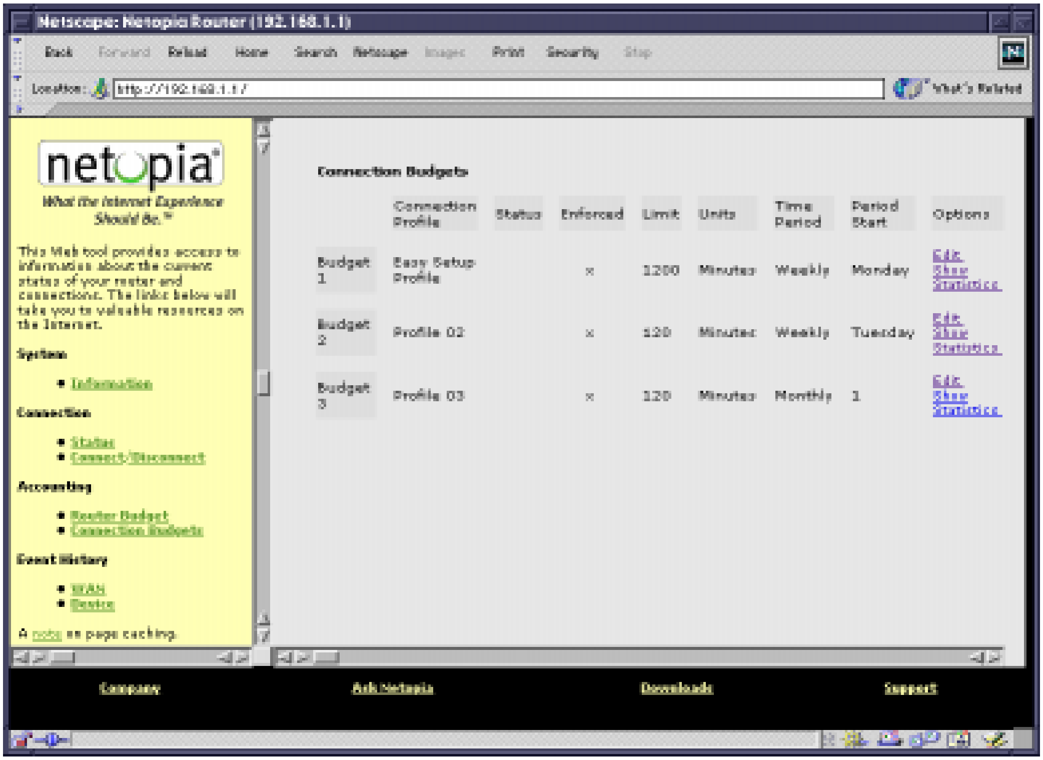
Total First Minutes. The number of first minutes of outbound calls to be placed during the recording interval for all your configured budgets

Total Additional Minutes. The total time of all outbound calls to be placed during the recording interval for all your configured budgets

Remaining Minutes. The time remaining during the recording interval for all your configured budgets

Connection Budgets page

The Connection Budgets page displays information for three budgets or Connection Profiles for tracking and controlling connection usage on a per-Connection Profile basis.



This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.

System

- Information

Connection

- Status
- Connect/Disconnect

Accounting

- Router Budget
- Connection Budgets

Event History

- WAN
- Device

A note on page caching.

Connection Budgets

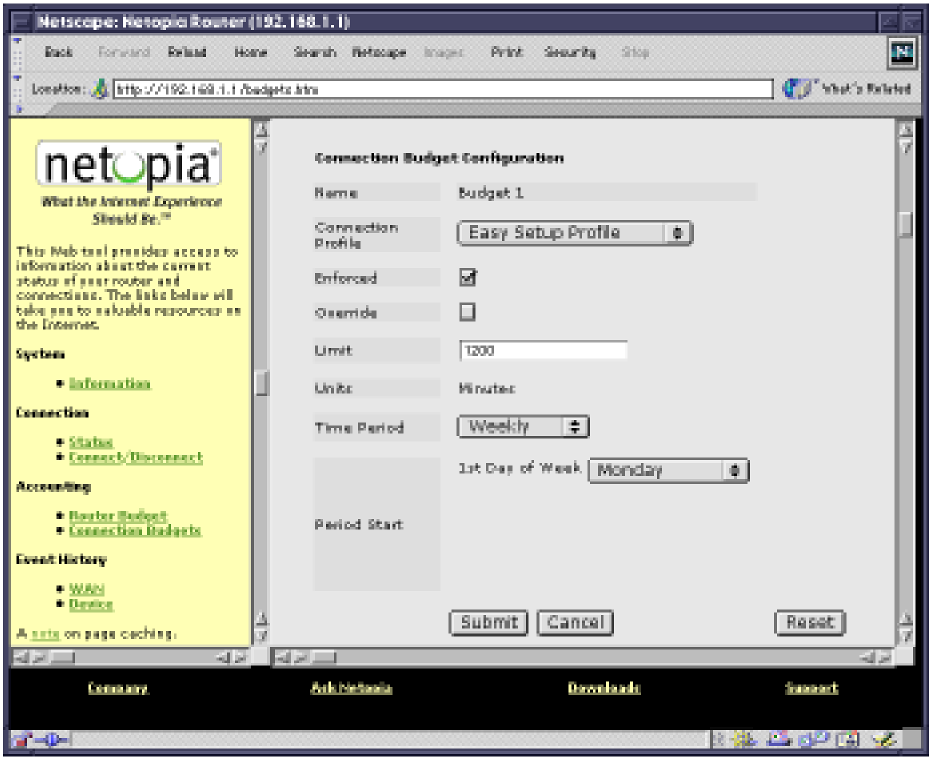
	Connection Profile	Status	Enforced	Limit	Units	Time Period	Period Start	Options
Budget 1	Easy Setup Profile		x	1200	Minutes	Weekly	Monday	Edit Show Statistics
Budget 2	Profile 02		x	120	Minutes	Weekly	Tuesday	Edit Show Statistics
Budget 3	Profile 03		x	120	Minutes	Monthly	1	Edit Show Statistics

The status of your Connection Budgets is summarized on this page.

You configure your budgets in the Budget Configuration page. To configure a budget, click the **Edit** link for that budget. The Connection Budget Configuration page appears. (See page 8-19.)

To view the statistics for each budget, click the **Show Statistics** link. The Budget Statistics page appears. (See page 8-20.)

Connection Budget Configuration page



This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.

Connection Budget Configuration

Name	Budget 1
Connection Profile	Easy Setup Profile
Enforced	☑
Override	□
Limit	1200
Units	Minutes
Time Period	Weekly
Period Start	1st Day of Week Monday

Submit Cancel Reset

You can configure budgets to be:

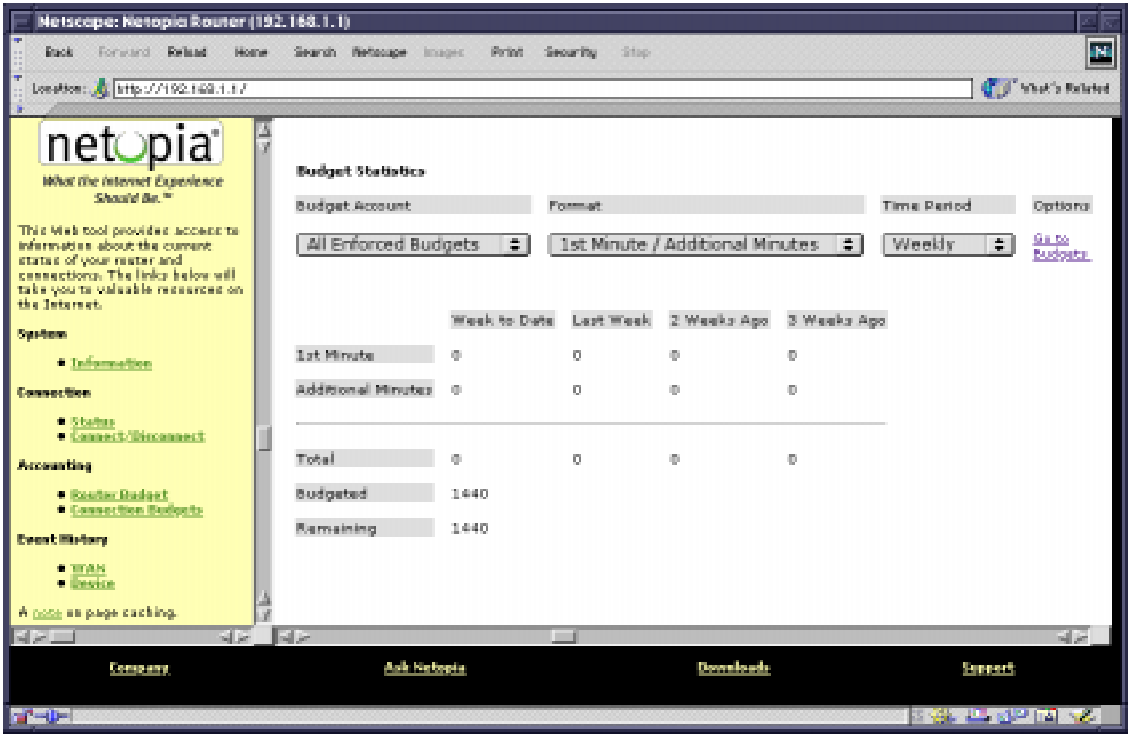
- **Enforced**, meaning that when you reach the usage limit for the assigned time period, the Connection Profile will allow no more connections. If the budget is not enforced, the system will merely keep track of its usage. To enforce this budget, check the **Enforced** checkbox.
- in **Override** mode. Checking this option allows you to exceed your budget during the current time period without tearing down active connections. At the end of the current time period this option is automatically deactivated. If you want to be able to exceed your enforced budget again, you must check this option for each new time period.

  Checking **Override** disables call blocking, even if the call is over its limit. The override flag is automatically reset to be off at the start of a new period. This is so that you don't need to disable **Enforced** to by-pass the limit and or remember to turn it back on when the new period starts.
- set to a predefined **Limit** of minutes of usage
- set to the **Time Period**, weekly or monthly, that you specify for your own budgeting requirements
- started on a specific day of the week or month by selecting the day you want to start from the pull-down menu. If you set a weekly schedule, you choose the day of the week to start it; if you set a monthly

schedule, you choose the day of the month to start it.

Click the **Submit** button to enable your entries and be returned to the Connection Budgets page or click the **Cancel** button to discard all your entries. Click the **Reset** button to reset all counters and archives to zero.

Budget Statistics page



This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.

System

- Information

Connection

- Status
- Connect/Disconnect

Accounting

- Router Budget
- Connection Budgets

Event History

- WAN
- Device

A note on page caching.

Budget Statistics

Budget Account	Format	Time Period	Options
All Enforced Budgets	1st Minute / Additional Minutes	Weekly	Go to Budgets

	Week to Date	Last Week	2 Weeks Ago	3 Weeks Ago
1st Minute	0	0	0	0
Additional Minutes	0	0	0	0
Total	0	0	0	0
Budgeted	1440			
Remaining	1440			

You can view statistics for all of your budgets at once or one at a time.

- To view the statistics for a single budget or all enforced budgets, select the budget you want to view from the **Budget Account** pull-down menu.
- Select the **Format** you want to view, either **1st Minute / Additional Minutes** or **Channel 1 / Channel 2**.
- Select the **Time Period** you want to view, either Weekly or Monthly.

The information display will immediately change to show the information you specified in the format you chose.

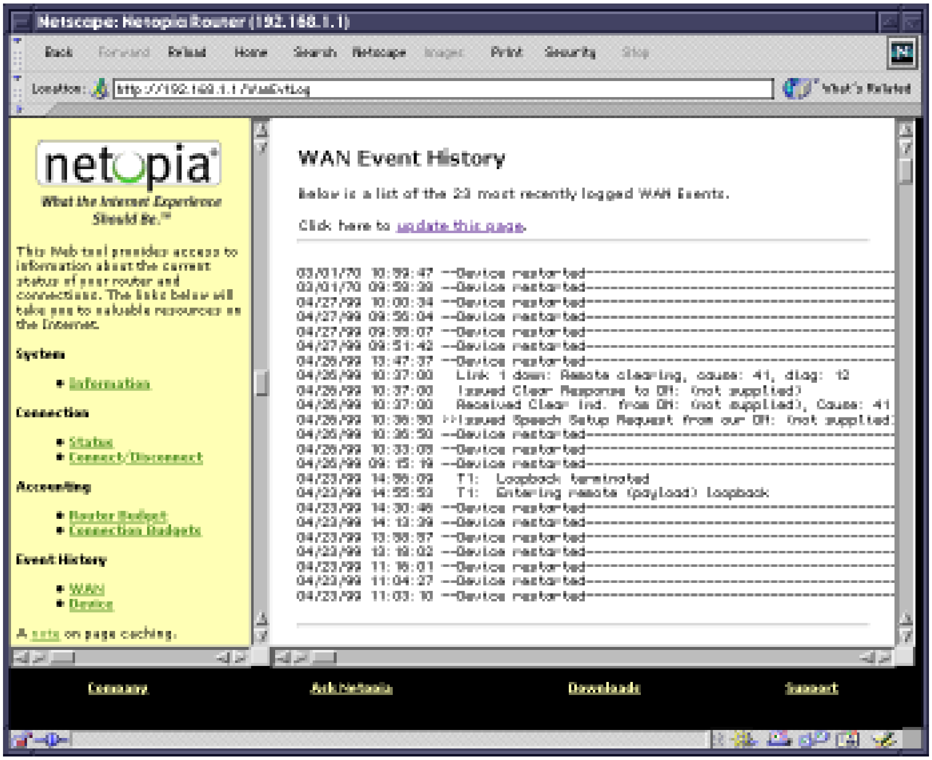
To return to the Connection Budgets page, click the **Go to Budgets** link.

Event History pages

The Netopia R2020 records certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the router's system and one for the WAN. The Netopia R2020's built-in battery backup prevents loss of event history from a shutdown or reset.

The router's event histories are structured to display the most recent events first and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk. Both the WAN Event History and Device Event History pages retain records of up to 128 of the most recent events.

WAN Event History page



This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.

A note on page caching.

WAN Event History

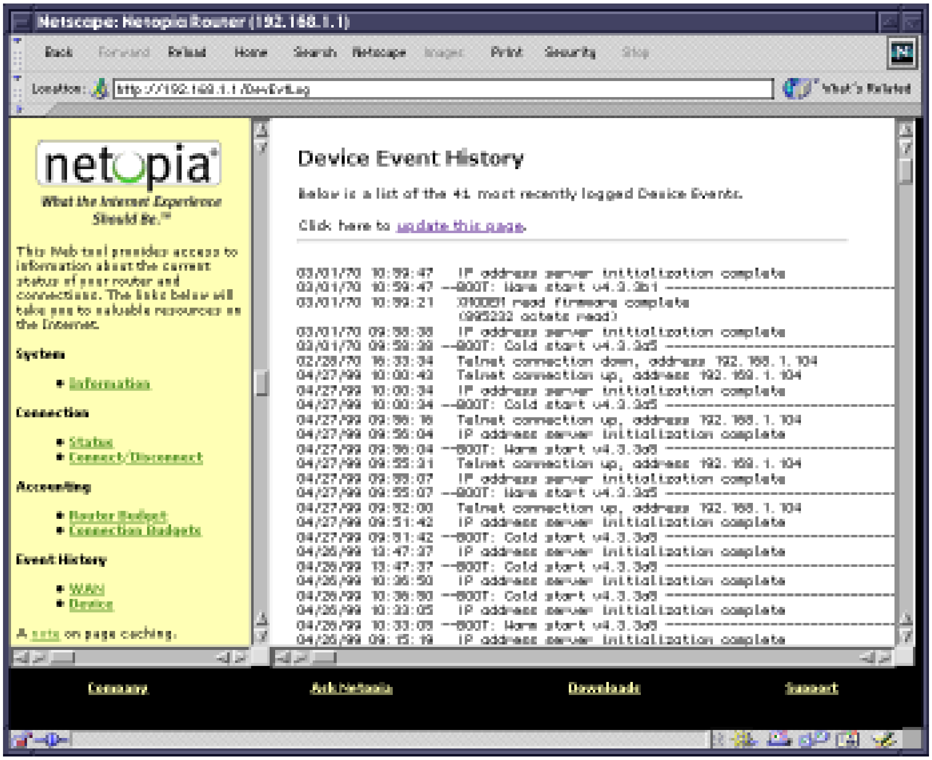
Below is a list of the 23 most recently logged WAN Events.

Click here to update this page.

```
03/01/70 10:59:47 --Device restarted-----------------------------------------
03/01/70 09:59:39 --Device restarted-----------------------------------------
04/27/99 10:00:34 --Device restarted-----------------------------------------
04/27/99 09:58:04 --Device restarted-----------------------------------------
04/27/99 09:55:07 --Device restarted-----------------------------------------
04/27/99 09:51:42 --Device restarted-----------------------------------------
04/26/99 13:47:37 --Device restarted-----------------------------------------
04/26/99 10:37:00   Link 1 down: Remote clearing, cause: 41, diag: 12
04/26/99 10:37:00   Issued Clear Response to DN: (not supplied)
04/26/99 10:37:00   Received Clear Ind. from DN: (not supplied), Cause: 41
04/26/99 10:36:50 **Issued Speech Setup Request from our DN: (not supplied)
04/26/99 10:36:50 --Device restarted-----------------------------------------
04/26/99 10:33:05 --Device restarted-----------------------------------------
04/26/99 09:15:19 --Device restarted-----------------------------------------
04/23/99 14:58:09   T1:  Loopback terminated
04/23/99 14:55:53   T1:  Entering remote (payload) loopback
04/23/99 14:30:46 --Device restarted-----------------------------------------
04/23/99 14:13:39 --Device restarted-----------------------------------------
04/23/99 13:55:57 --Device restarted-----------------------------------------
04/23/99 13:19:02 --Device restarted-----------------------------------------
04/23/99 11:16:01 --Device restarted-----------------------------------------
04/23/99 11:04:27 --Device restarted-----------------------------------------
04/23/99 11:03:10 --Device restarted-----------------------------------------
```

You can refresh the WAN Event History log by clicking the **update this page** link.

Device Event History page


Netscape: Netopia Router (192.168.1.1)
Back
Forward
Reload
Home
Search
Netscape
Images
Print
Security
Shop
Location:
http://192.168.1.1/DevEvLog
What's Related
netopia
What the Internet Experience Should Be.™

This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.

System

- Information

Connection

- Status
- Connect/Disconnect

Accounting

- Router Budget
- Connection Budgets

Event History

- WAN
- Device

A note on page caching.

Device Event History

Below is a list of the 41 most recently logged Device Events.

Click here to update this page.

```
03/01/70 10:59:47   IP address server initialization complete
03/01/70 10:59:47 --BOOT: Warm start v4.3.3b1 ---------------------------
03/01/70 10:59:21   XMODEM read firmware complete
                    (995232 octets read)
03/01/70 09:58:38   IP address server initialization complete
03/01/70 09:58:38 --BOOT: Cold start v4.3.3a5 ---------------------------
02/28/70 16:33:34   Telnet connection down, address 192.168.1.104
04/27/99 10:00:43   Telnet connection up, address 192.168.1.104
04/27/99 10:00:34   IP address server initialization complete
04/27/99 10:00:34 --BOOT: Cold start v4.3.3a5 ---------------------------
04/27/99 09:58:16   Telnet connection up, address 192.168.1.104
04/27/99 09:56:04   IP address server initialization complete
04/27/99 09:56:04 --BOOT: Warm start v4.3.3a5 ---------------------------
04/27/99 09:55:31   Telnet connection up, address 192.168.1.104
04/27/99 09:55:07   IP address server initialization complete
04/27/99 09:55:07 --BOOT: Warm start v4.3.3a5 ---------------------------
04/27/99 09:52:00   Telnet connection up, address 192.168.1.104
04/27/99 09:51:42   IP address server initialization complete
04/27/99 09:51:42 --BOOT: Cold start v4.3.3a5 ---------------------------
04/26/99 13:47:37   IP address server initialization complete
04/26/99 13:47:37 --BOOT: Cold start v4.3.3a5 ---------------------------
04/26/99 10:36:50   IP address server initialization complete
04/26/99 10:36:50 --BOOT: Cold start v4.3.3a5 ---------------------------
04/26/99 10:33:05   IP address server initialization complete
04/26/99 10:33:05 --BOOT: Warm start v4.3.3a5 ---------------------------
04/26/99 09:15:19   IP address server initialization complete
```

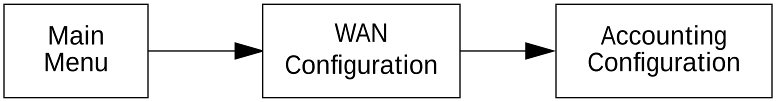
Company   Ask Netopia   Downloads   Support

You can refresh the Device Event History log by clicking the **update this page** link.

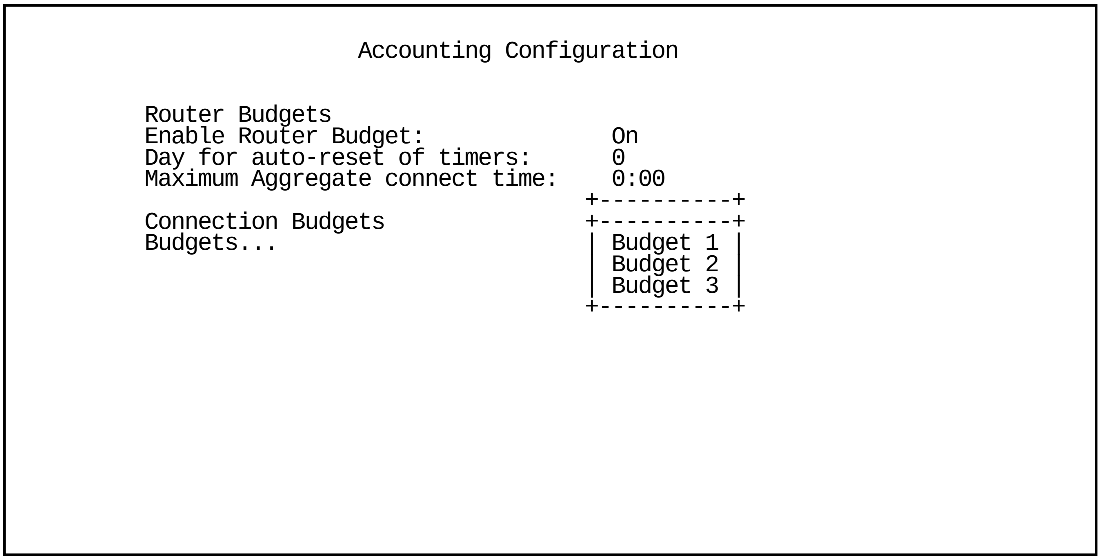
Console-based management screens

You access the console-based management screens either by running your Telnet application or your terminal emulator to the serial console. For details on how to do this, see Chapter 5, “Console-based Management.”

Navigate to the Accounting screens.



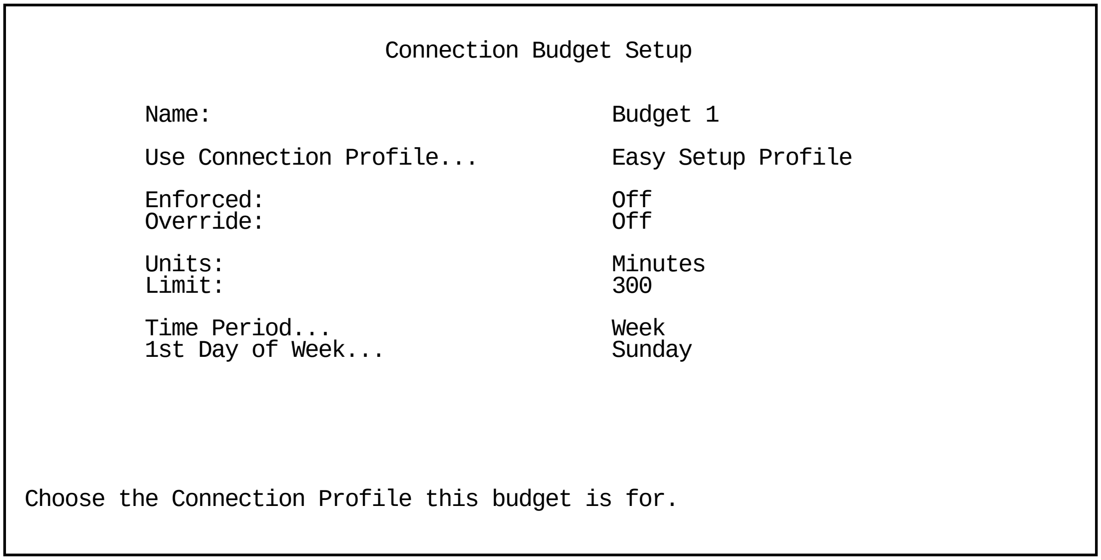
The Accounting Configuration screen appears.



```
                Accounting Configuration


Router Budgets
Enable Router Budget:              On
Day for auto-reset of timers:      0
Maximum Aggregate connect time:    0:00
                                 +----------+
Connection Budgets               +----------+
Budgets...                       | Budget 1 |
                                 | Budget 2 |
                                 | Budget 3 |
                                 +----------+
```

To edit your budgets select **Budgets**, and from the pop-up menu, select the budget you want to edit.

The Budget Setup screen appears.



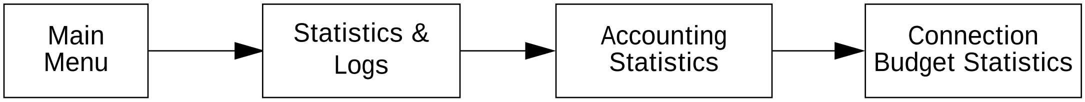
```
                         Connection Budget Setup

        Name:                             Budget 1

        Use Connection Profile...         Easy Setup Profile

        Enforced:                         Off
        Override:                         Off

        Units:                            Minutes
        Limit:                            300

        Time Period...                    Week
        1st Day of Week...                Sunday




Choose the Connection Profile this budget is for.
```

Configuration is similar to the Web-based management configuration screens.

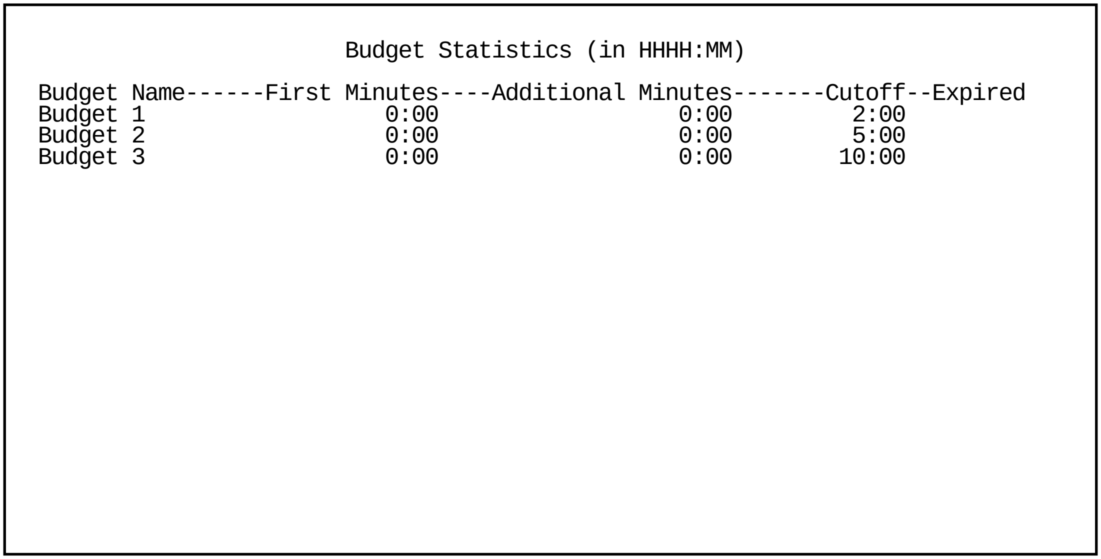
- Selecting **Use Connection Profile** displays a pop-up list of all of your Connection Profiles. Choose the Connection Profile you want this budget to apply to and press Return.
- Toggle **Enforced** to either **On** or **Off** to enforce whether the connection is torn down when the budget limit is reached.
- Toggle **Override** to either **On** or **Off**. With Override on you can exceed your budget during the current time period without tearing down active connections. At the end of the current time period this option is automatically deactivated. If you want to be able to exceed your enforced budget again, you must toggle this option to On for each new time period.

  Toggling **Override** to On disables call blocking, even if the call is over its limit. The override flag is automatically reset to be Off at the start of a new period. This is so that you don’t need to disable **Enforced** to by-pass the limit or remember to turn it back on when the new period starts.
- The **Units** field is not editable.
- In the **Limit** field enter the number of minutes your budget allows.
- From the **Time Period** pop-up menu select either **Week** or **Month**, depending on your budgeting requirements.
- If you set the time period to Week, from the **1st Day of Week** pop-up menu select the day of the week on which your budget starts, or
  if you set the time period to Month, from the **1st Day of Month** pop-up menu select the day of the month on which your budget starts.

You can monitor your usage against your budget by reviewing the Connection Budget Statistics screen in the Accounting Statistics. From the Main Menu navigate to the Connection Budget Statistics screen.



The Budget Statistics screen appears.



```
                       Budget Statistics (in HHHH:MM)

Budget Name------First Minutes----Additional Minutes-------Cutoff--Expired
Budget 1                  0:00                  0:00         2:00
Budget 2                  0:00                  0:00         5:00
Budget 3                  0:00                  0:00        10:00
```

You can view statistics for all your budgets at once or one at a time.

- **Budget Name** shows the names of your budgets.
- **First Minutes** displays the number of first minutes of outbound calls placed during the recording interval.
- **Additional Minutes** displays the remaining time of all outbound calls placed during the recording interval.
- **Cutoff** displays the number of hours budgeted for this Connection Profile.
- **Expired** displays the amount of time used against the budgeted amount.

To clear the counters and reset the statistics, use the down arrow key to select a budget and press Return. A pop-up window will ask you to confirm that you want to clear this budget’s statistics. You can cancel if you change your mind.

To return to the Accounting Statistics screen, press Escape.

Date and time setting

Note: If you have Connection Budgets configured, changing the date setting will reset the Connection Budgets under one of the following conditions:

- If the new date is greater than the old date and the new date falls outside of the current budget window; or
- If the new date is in the past and the date is not the current date (i.e., yesterday or earlier).

A warning message is displayed in the console window when a budget is reset.

See "Date and Time" on page 7-11 for more information on setting the date and time.

Chapter 9

Virtual Private Networks

The Netopia R2020 Dual Analog Router offers both PPTP and ATMP Layer 2 tunneling support for Virtual Private Networks (VPN) as a component of a connection profile.

Overview

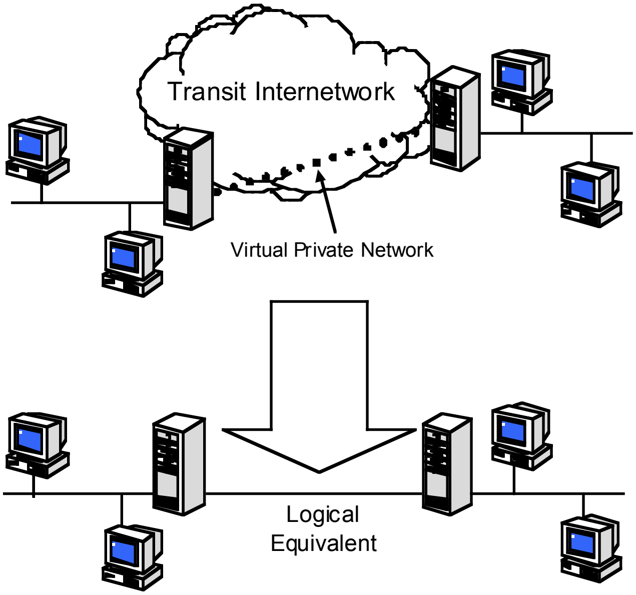
When you make a long distance telephone call from your home to a relative far away, you are creating a private network. You can hold a conversation, and exchange information about the happenings on opposite sides of the state, or the continent, that you are mutually interested in. When your next door neighbor picks up the phone to call her daughter at college, at the same time you are talking to your relatives, your calls don't overlap, but each is separate and private. Neither house has a direct wire to the places they call. Both share the same lines on the telephone poles (or underground) on the street.

These calls are *virtual private networks*. *Virtual*, because they appear to be direct connections between the calling and answering parties, even though they travel over the public wires and switches of the phone company; *private*, because neither pair of calling and answering parties interacts with the other; and *networks*, because they exchange information.

Computers can do the same thing; it's called Virtual Private Networks (VPNs). Equipped with Netopia Routers running the version 4.4 firmware, a single computer or private network (LAN) can establish a private connection with another computer or private network over the public network (Internet).

The Netopia Router can be used in VPNs either to initiate the connection or to answer it. When used in this way, the routers are said to be *tunnelling* through the public network (Internet). The advantages are that, like your long distance phone call, you don't need a direct line between one computer or LAN and the other, but use the local connections, making it much cheaper; and the information you exchange through your tunnel is private and secure.

Tunneling is a process of creating a private path between a remote user or private network and another private network over some intermediate network, such as the IP-based Internet. A VPN allows remote offices or employees access to your internal business LAN through means of encryption allowing the use of the public Internet to look “virtually” like a private secure network. When two networks communicate with each other through a network based on the Internet Protocol, they are said to be *tunneling* through the IP network.



Unlike the phone company, private and public computer networks can use more than one protocol to carry your information over the wires. Two such protocols are in common use for tunnelling, Point-to-Point Tunnelling Protocol (PPTP) and Ascend Tunnel Management Protocol (ATMP). The Netopia Router can use either one.

- Point-to-Point Tunneling Protocol (PPTP) is an extension of Point-to-Point Protocol (PPP) and uses a client and server model. Netopia's PPTP implementation is compatible with Microsoft's and can function as either the client (PAC) or the server (PNS). As a client, a Netopia R-series router can provide all users on a LAN with secure access over the Internet to the resources of another LAN by setting up a tunnel with a Windows NT server running Remote Access Services (RAS) or with another Netopia Router. As a server, a Netopia R-series router can provide remote users a secure connection to the resources of the LAN over a dial-up, cable, DSL, or any other type of Internet access. Because PPTP can create a VPN tunnel using the Dial-Up Networking (DUN) (see "Dial-Up Networking for VPN" on page 9-10) utility built into Windows 95, 98, or NT, no additional client software is required.
- Ascend Tunnel Management Protocol (ATMP) is the protocol that is implemented in many Ascend routers. ATMP is a simple protocol for connecting nodes and/or networks together over the Internet via a tunnel. ATMP encapsulates IP or other user data without PPP headers within General Routing Encapsulation (GRE) protocol over IP. ATMP is more efficient than PPTP for network-to-network tunnels.

When used to initiate the tunnelled connection, the Netopia Router is called a *PPTP Access Concentrator* (*PAC*, in PPTP language), or a *foreign agent* (in ATMP language). When used to answer the tunnelled connection, the Netopia Router is called a *PPTP Network Server* (*PNS*, in PPTP language) or a *home agent* (in ATMP language).

In either case, the Netopia Router wraps, or encapsulates, information that one end of the tunnel exchanges with the other, in a wrapper called General Routing Encapsulation (GRE), at one end of the tunnel, and unwraps, or decapsulates, it at the other end.

Configuring the Netopia Router for use with either of the two protocols is done through the console-based menu screens. Each type is described in its own section:

- "About PPTP tunnels" on page 9-4
- "About ATMP Tunnels" on page 9-16

Your configuration depends on which protocol you (and the router at the other end of your tunnel) will use, and whether or not you will be using the VPN client software in a standalone remote connection.

Summary

A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing you to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks.

VPNs allow networks to communicate across an IP network. Your local networks (connected to the Netopia Router) can exchange data with remote networks that are also connected to a VPN-capable router.

This feature provides individuals at home, on the road, or in branch offices with a cost-effective and secure way to access resources on remote LANs connected to the Internet with Netopia Routers. The feature is built around two key technologies: PPTP and ATMP.

About PPTP tunnels

To set up a PPTP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote PPTP partner. You use the same procedure to initiate a PPTP tunnel that terminates at a remote PPTP server or to terminate a tunnel initiated by a remote PPTP client.

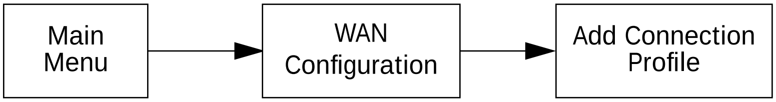
PPTP Configuration

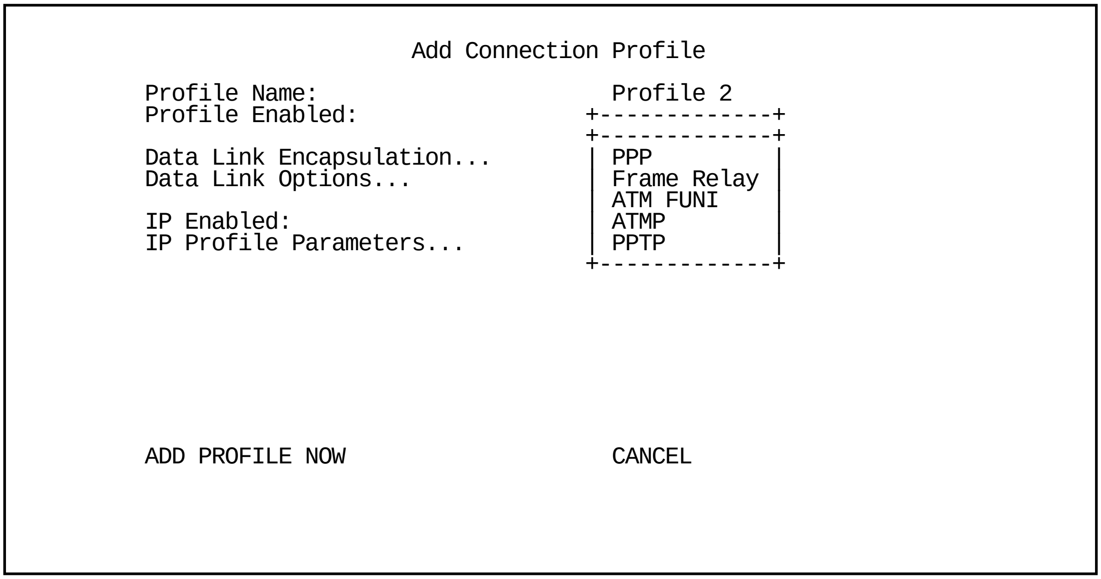
To set up the router as a PPTP Network Server (PNS) capable of answering PPTP tunnel requests you must also configure the VPN Default Answer Profile. See "VPN Default Answer Profile" on page 9-8 for more information.

PPTP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, as PPTP is not a native encapsulation. Consequently, the Easy Setup Profile does not offer PPTP datalink encapsulation. See "Creating a new Connection Profile" on page 7-2 for information on creating Connection Profiles.

Channel 4 (and higher) events, such as connections and disconnections, reported in the WAN Event Histories are VPN tunnel events.

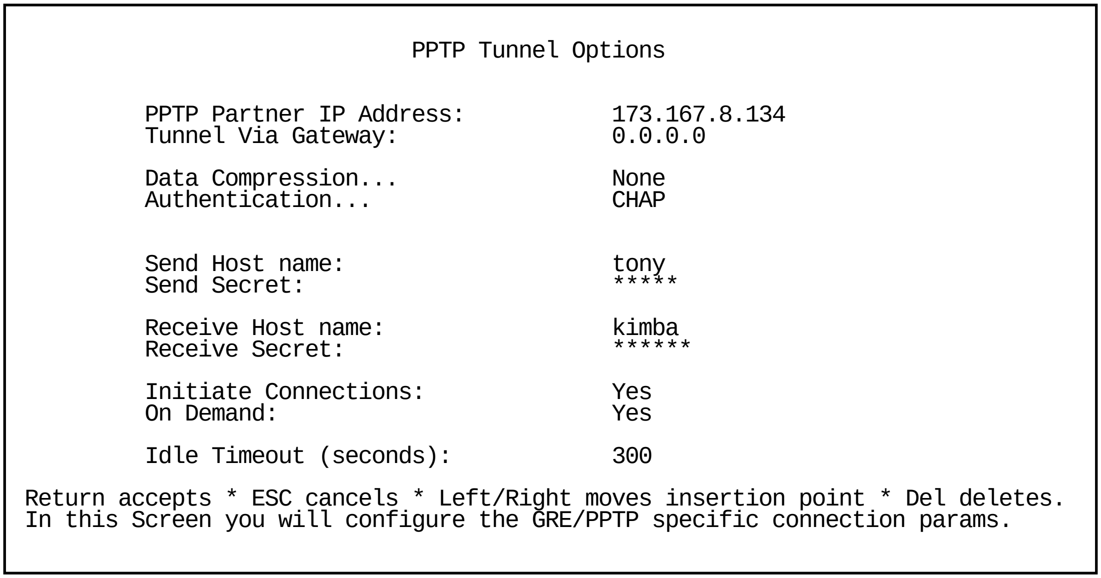
To define a PPTP tunnel, navigate to the Add Connection Profile menu from the Main Menu.





```
                    Add Connection Profile

     Profile Name:                      Profile 2
     Profile Enabled:                 +-------------+
                                      +-------------+
     Data Link Encapsulation...       | PPP         |
     Data Link Options...             | Frame Relay |
                                      | ATM FUNI    |
     IP Enabled:                      | ATMP        |
     IP Profile Parameters...         | PPTP        |
                                      +-------------+





     ADD PROFILE NOW                    CANCEL
```

When you define a Connection Profile as using PPTP by selecting PPTP as the datalink encapsulation method, and then select **Data Link Options**, the PPTP Tunnel Options screen appears.



```
                              PPTP Tunnel Options

         PPTP Partner IP Address:          173.167.8.134
         Tunnel Via Gateway:               0.0.0.0

         Data Compression...               None
         Authentication...                 CHAP


         Send Host name:                   tony
         Send Secret:                      *****

         Receive Host name:                kimba
         Receive Secret:                   ******

         Initiate Connections:             Yes
         On Demand:                        Yes

         Idle Timeout (seconds):           300

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
In this Screen you will configure the GRE/PPTP specific connection params.
```

Note: Profiles using PPTP do not offer a Telco Options screen.

- Enter the **PPTP Partner IP Address**. This specifies the address of the other end of the tunnel.

  If you do not specify the PPTP Partner IP Address the gateway cannot initiate tunnels, i.e., act as a PPTP Access Concentrator (PAC) for this profile. It can only accept tunnel requests as a PPTP Network Server (PNS).

- If you specify the PPTP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, the **Tunnel Via Gateway** option becomes visible. You can enter the address by which the gateway partner is reached.

  If you do not specify the PPTP Partner IP Address, the router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e. the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.

- You can specify a **Data Compression** algorithm, either None or Standard LZS, for the PPTP connection.

  Note: When the Authentication protocol is MS-CHAP, compression is set to None, and the **Data Compression** option is hidden.

- From the pop-up menu select an **Authentication** protocol for the PPP connection. Options are PAP, CHAP, or MS-CHAP. The default is PAP. The authentication protocol must be the same on both ends of the tunnel.

- When the authentication protocol is MS-CHAP, you can specify a **Data Encryption** algorithm for the PPTP connection. Available options are MPPE and None (the default). For other authentication protocols, this option is hidden. When MPPE is negotiated, the WAN Event History reports that it is negotiated as a CCP (compression) type. This is because the MPPE protocol uses a compression engine, even though it is not itself a compression protocol.

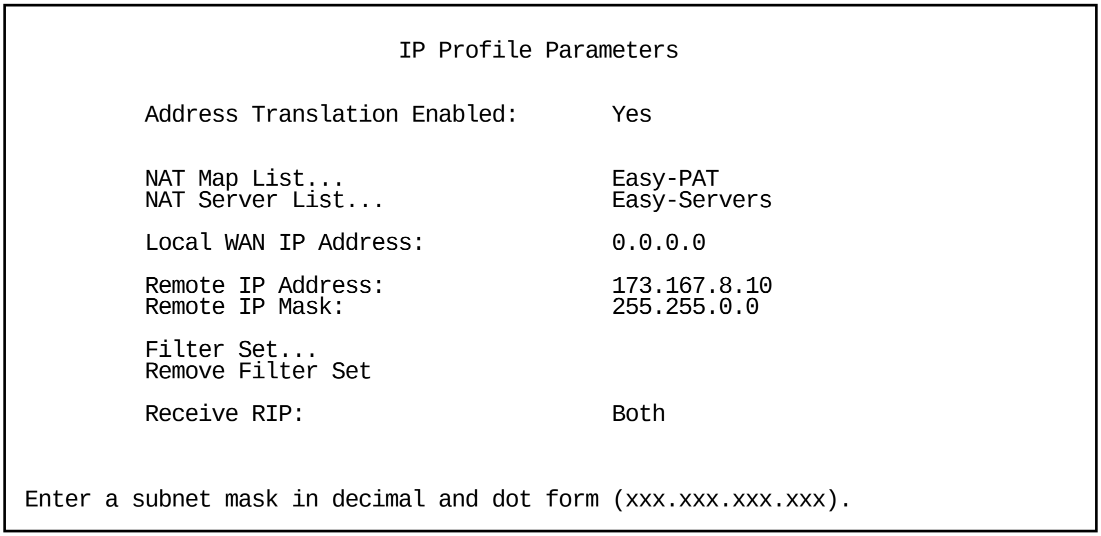
- You can specify a **Send Host Name** which is used with Send Secret for authenticating with a remote PNS when the profile is used for initiating a tunnel connection.

- You must specify a **Send Secret** (the CHAP term for password), used for authenticating the tunnel when initiating a tunnel connection.

- You can specify a **Receive Host Name** which is used with the Receive Secret for authenticating a remote PPTP client.
- You must specify a **Receive Secret**, used for authenticating the remote PPTP client.
- You can specify that this router will **Initiate Connections** (acting as a PAC) or only answer them (acting as a PNS).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established via the call management screens or may be scheduled using the scheduled connections feature. See "Scheduled Connections" in the *User's Reference Guide*.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.

  An alternate way to force a tunnel to stay up is to define a forced up scheduled connection for the profile. For more information, see "Scheduled connections" on page 8-7.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return.

  The IP Profile Parameters screen appears.



```
                             IP Profile Parameters

         Address Translation Enabled:       Yes


         NAT Map List...                    Easy-PAT
         NAT Server List...                 Easy-Servers

         Local WAN IP Address:              0.0.0.0

         Remote IP Address:                 173.167.8.10
         Remote IP Mask:                    255.255.0.0

         Filter Set...
         Remove Filter Set

         Receive RIP:                       Both


Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).
```

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

Note: A peculiarity associated with VPNs is that when a PAC has NAT applied to a Connection Profile set for PPTP data link encapsulation, the PNS and devices behind it, cannot Ping the PAC's tunnel end-point IP address. This is because ICMP packets have no port association, and thus will be discarded rather than being processed by NAT.

Ordinarily, Ping is an excellent troubleshooting tool, but it will not be effective in this circumstance. Instead, use another TCP- or UDP-based network service for troubleshooting. Since the Netopia Router is capable of serving Telnet and HTTP, we recommend using these services instead of Ping.

Encryption support

Encryption is a method for altering user data into a form that is unusable by anyone other than the intended recipient. The recipient must have the means to decrypt the data to render it usable to them. The encryption process protects the data by making it difficult for any third party to get at the original data.

Netopia PPTP is fully compatible with Microsoft Point-to-Point Encryption (MPPE) data encryption for user data transfer over the PPTP tunnel. Microsoft Windows NT Server provides MPPE encryption capability only when Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is enabled. Netopia complies with this feature to allow MPPE only when MS-CHAP is negotiated. MS-CHAP and MPPE are user-selectable options in the PPTP Tunnel Options screen. If either the client or the server side specifies encryption, then encryption becomes mandatory for both.

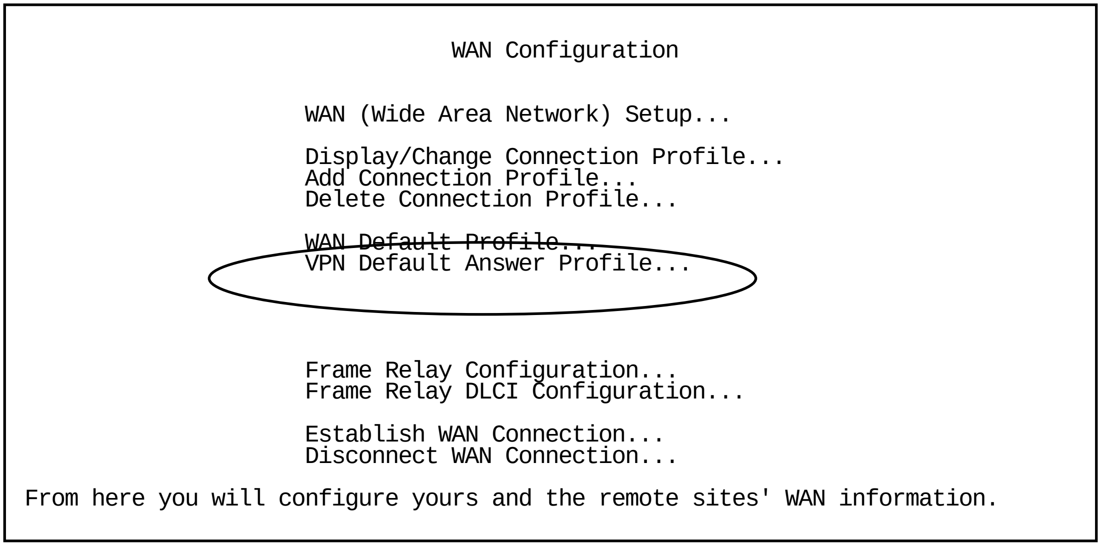
Netopia’s ATMP implementation supports Data Encryption Standard (DES) data encryption for user data transfer over the ATMP tunnel between two Netopia routers. The encryption option, none or DES, is a selectable option in the ATMP Tunnel Options screen.

Notes:

- Do not set your NT Server to enforce MS-CHAP V2, as the router does not currently support MS-CHAP V2.
- Do not set your NT Server to “Require strong data encryption” in RAS Network Configuration, as the router does not currently support 128-bit encryption.

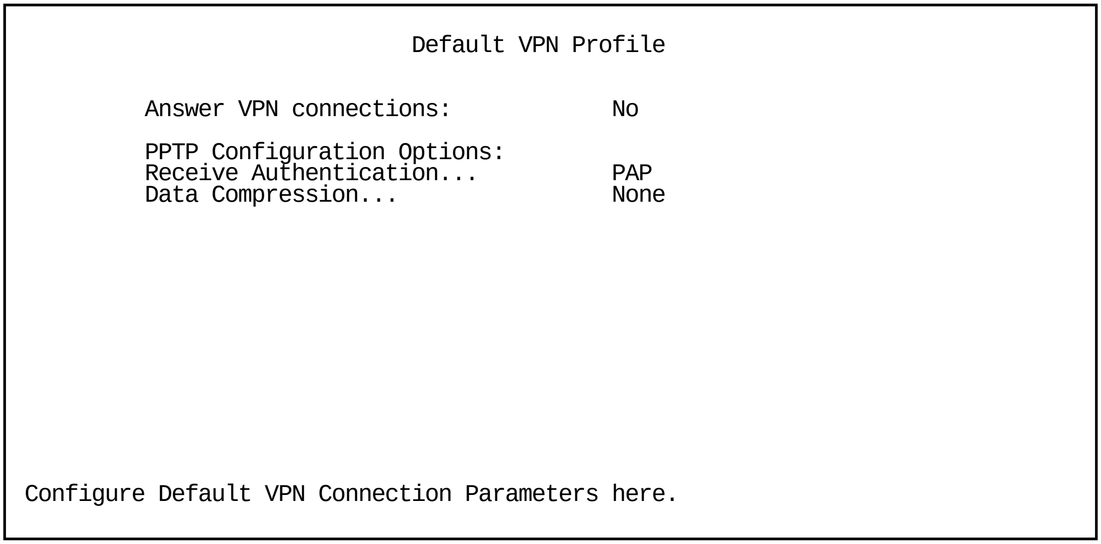
VPN Default Answer Profile

The WAN Configuration menu offers a VPN Default Answer Profile option. Use this selection when your router is acting as the server for VPN connections, that is, when you are on the answering end of the tunnel establishment. The VPN Default Answer Profile determines the way the attempted tunnel connection is answered.



```
                                 WAN Configuration

                      WAN (Wide Area Network) Setup...

                      Display/Change Connection Profile...
                      Add Connection Profile...
                      Delete Connection Profile...

                      WAN Default Profile...
                      VPN Default Answer Profile...



                      Frame Relay Configuration...
                      Frame Relay DLCI Configuration...

                      Establish WAN Connection...
                      Disconnect WAN Connection...

 From here you will configure yours and the remote sites' WAN information.
```

To set the parameters under which the router will answer attempted VPN connections, select **VPN Default Answer Profile** and press Return. The Default VPN Profile screen appears.



```
                              Default VPN Profile

          Answer VPN connections:            No

          PPTP Configuration Options:
          Receive Authentication...          PAP
          Data Compression...                None









 Configure Default VPN Connection Parameters here.
```

- Toggle **Answer VPN Connections** to **Yes** if you want the router to accept VPN connections or **No** (the default) if you do not. This applies to both ATMP and PPTP connections.

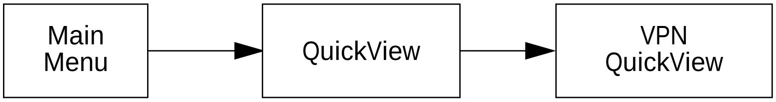
- For PPTP tunnel connections only, you must define what type of authentication these connections will use. Select **Receive Authentication** and press Return. A pop-up menu offers the following options: PAP (the default), CHAP, or MS-CHAP.
- If you chose PAP or CHAP authentication, from the **Data Compression** pop-up menu select either None (the default) or Standard LZS.

  If you chose MS-CHAP authentication, the **Data Compression** option is not required, and this menu item becomes hidden.

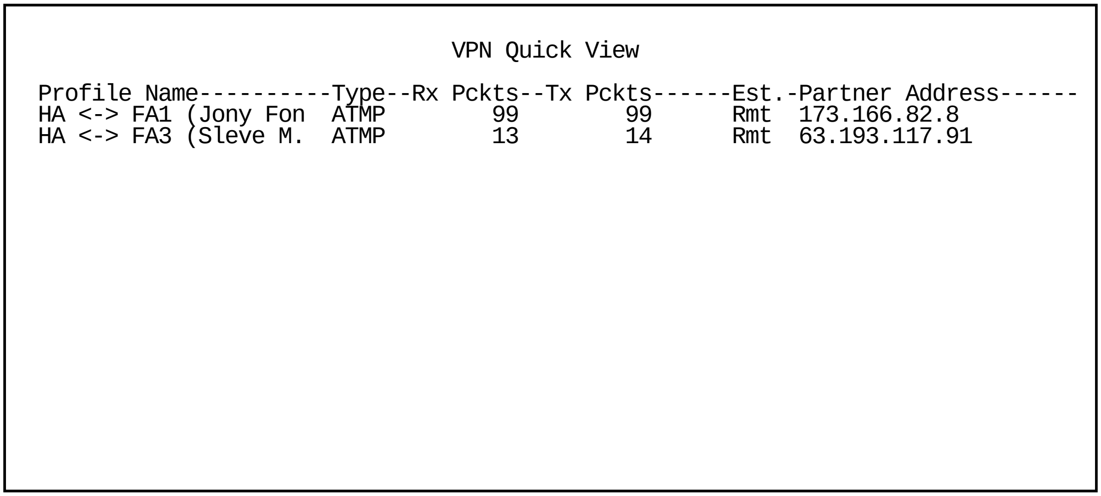
VPN QuickView

You can view the status of your VPN connections in the VPN QuickView screen.

From the Main Menu select QuickView and then VPN QuickView.



The VPN QuickView screen appears.



```
                               VPN Quick View

Profile Name----------Type--Rx Pckts--Tx Pckts------Est.-Partner Address------
HA <-> FA1 (Jony Fon  ATMP        99        99      Rmt  173.166.82.8
HA <-> FA3 (Sleve M.  ATMP        13        14      Rmt  63.193.117.91
```

Profile Name: Lists the name of the Connection Profile being used, if any.

Type: Shows the data link encapsulation method (PPTP or ATMP).

Rx Pckts: Shows the number of packets received via the VPN tunnel.

Tx Pckts: Shows the number of packets transmitted via the VPN tunnel.

Est: Indicates whether the connection was locally (“Lcl”) or remotely (“Rmt”) established.

Partner Address: Shows the tunnel partner’s IP address.

Dial-Up Networking for VPN

Microsoft Windows Dial-Up Networking software permits a remote stand-alone workstation to establish a VPN tunnel to a PPTP server such as a Netopia Router located at a central site. Dial-Up Networking also allows a mobile user who may not be connected to a PAC to dial into an intermediate ISP and establish a VPN tunnel to, for example, a corporate headquarters, remotely. Netopia Routers also can serve as a PAC at the workstation's site, making it unnecessary for the standalone workstation to initiate the tunnel. In such a case, the Dial-Up Networking software is not required, since the Netopia Router initiates the tunnel.

This section is provided for users who may require the VPN client software for Dial-Up Networking in order to connect to an ISP who provides a PPTP account.

Microsoft Windows Dial-Up Networking (DUN) is the means by which you can initiate a VPN tunnel between your individual remote client workstation and a private network such as your corporate LAN via the Internet. DUN is a software adapter that allows you to establish a tunnel.

DUN is a free add-on available for Windows 95, and comes standard with Windows 98 and Windows NT. The VPN tunnel behaves as a private network connection, unrelated to other traffic on the network. Once you have installed Dial-Up Networking, you will be able to connect to your remote site as if you had a direct private connection, regardless of the intervening network(s) through which your data passes. You may need to install the Dial-Up Networking feature of Windows 95, 98, or 2000 to take advantage of the virtual private networking feature of your Netopia router.

Note: For the latest information and tech notes on Dial-Up Networking and VPNs be sure to visit the Netopia website at http://www.netopia.com and, for the latest software and release notes, the Microsoft website at http://www.microsoft.com.

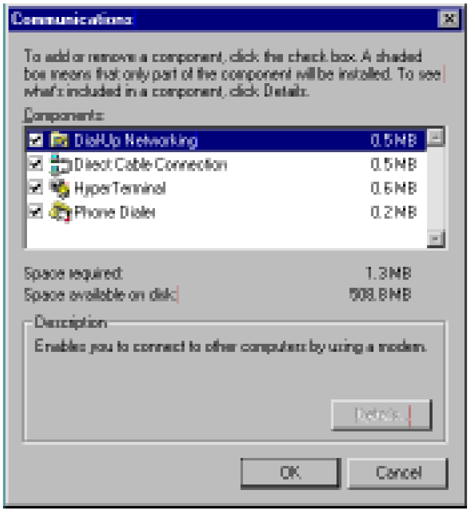
Installing Dial-Up Networking

Check to see if Dial-Up Networking is already installed on your PC. Open your My Computer (or whatever you have named it) icon on your desktop. If there is a folder named Dial-Up Networking, you don’t have to install it. If there is no such folder, you must install it from your system disks or CDROM. Do the following:

1. From the **Start** menu, select **Settings** and then **Control Panel**.
2. In the Control Panel window, double-click the **Add/Remove Programs** icon.

   The Add/Remove Programs Properties window appears.
3. Click the **Windows Setup** tab.
4. Double-click **Communications**.

The Communications window appears.



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑ Dial-Up Networking	0.5 MB
☑ Direct Cable Connection	0.5 MB
☑ HyperTerminal	0.6 MB
☑ Phone Dialer	0.2 MB

Space required:	1.3 MB
Space available on disk:	508.8 MB

Description

Enables you to connect to other computers by using a modem.

5. In the Communications window, select **Dial-Up Networking** and click the **OK** button.

   This returns you to the Windows Setup screen. Click the **OK** button.

6. Respond to the prompts to install Dial-Up Networking from the system disks or CDROM.

7. When prompted, reboot your PC.

Creating a new Dial-Up Networking profile

A Dial-Up Networking profile is like an address book entry that contains the information and parameters you need for a secure private connection. You can create this profile by using either the Internet Connection Wizard or the Make New Connection feature of Dial-Up Networking. The following instructions tell you how to create the profile with the Make New Connection feature. Do the following:

1. Double-click the **My Computer** (or whatever you have named it) icon on your desktop.

   Open the Dial-Up Networking folder, and then double-click **Make New Connection**. The Make New Connection wizard window appears.

2. Type a name for this connection (such as the name of your company, or the computer you are dialing into).

   From the pull-down menu, select the device you intend to use for the virtual private network connection. This can be any device you have installed or connected to your PC. Click the **Next** button. A screen appears with fields for you to enter telephone numbers for the computer you want to connect to.

3. Type the directory number or the **Virtual Circuit Identifier** number.

   This number is provided by your ISP or corporate administrator. Depending on the type of device you are using, the number may or may not resemble an ordinary telephone directory number.

4. Click the **Next** button.

   The final window will give you a chance to accept or change the name you have entered for this profile. If you are satisfied with it, click the **Finish** button. Your profile is complete.

Configuring a Dial-Up Networking profile

Once you have created your Dial-Up Networking profile, you configure it for TCP/IP networking to allow you to connect to the Internet through your Internet connection device. Do the following:

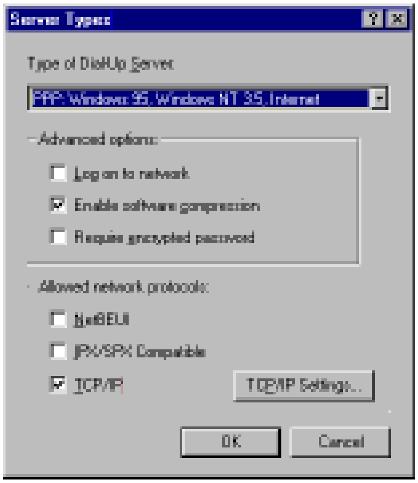
1. Double-click the **My Computer** (or whatever you have named it) icon on your desktop.

   Open the Dial-Up Networking folder. You will see the icon for the profile you created in the previous section.

2. Right-click the icon and from the pop-up menu select **Properties**.

3. In the Properties window click the **Server Type** button.

   From the Type of Dial-up Server pull-down menu select the appropriate type of server for your system version:



Server Types

Type of Dial-Up Server:

PPP: Windows 95, Windows NT 3.5, Internet

Advanced options:

□ Log on to network

☑ Enable software compression

□ Require encrypted password

Allowed network protocols:

□ NetBEUI

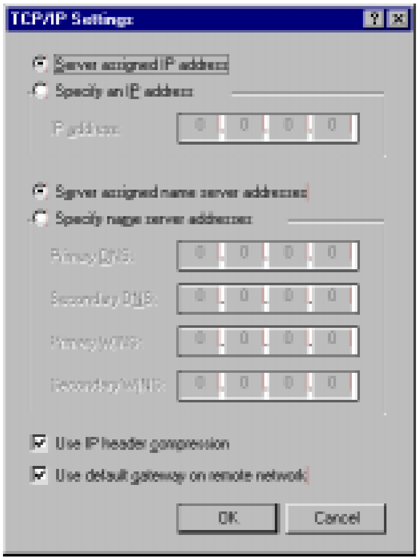
□ IPX/SPX Compatible

☑ TCP/IP

- Windows 95 users select **PPP: Windows 95, Windows NT 3.5, Internet**
- Windows 98 users select **PPP: Windows 98, Windows NT Server, Internet**

In the Allowed network protocols area check **TCP/IP** and uncheck all of the other checkboxes.

4. Click the **TCP/IP Settings** button.



TCP/IP Settings

● Server assigned IP address
○ Specify an IP address

IP address: 0 . 0 . 0 . 0

● Server assigned name server addresses
○ Specify name server addresses

Primary DNS: 0 . 0 . 0 . 0
Secondary DNS: 0 . 0 . 0 . 0
Primary WINS: 0 . 0 . 0 . 0
Secondary WINS: 0 . 0 . 0 . 0

☑ Use IP header compression
☑ Use default gateway on remote network

- If your ISP uses dynamic IP addressing (DHCP), select the Server assigned IP address radio button.
- If your ISP uses static IP addressing, select the Specify an IP address radio button and enter your assigned IP address in the fields provided. Also enter the IP address in the Primary and Secondary DNS fields.

5. Click the **OK** button in this window and the next two windows.

Installing the VPN Client

Before Installing the VPN Client you must have TCP/IP installed and have an established Internet connection.

Windows 95 VPN installation

1. From your Internet browser navigate to the following URL:

   http://www.microsoft.com/NTServer/nts/downloads/recommended/dunl3win95/releasenotes.aso

   Download the Microsoft Windows 95 VPN patch dun 1.3 to the Windows 95 computer you intend to use as a VPN client with PPTP. Follow the installation instructions.

2. From the Windows 95 **Start** menu select **Settings**, then **Control Panel** and click once.

   The Control Panel screen appears.

3. Double-click **Add/Remove Programs**.

   The Add/Remove Programs screen appears.

4. Click the **Windows Setup** tab.

   The Windows Setup screen will be displayed within the top center box.

5. Highlight **Communications** and double-click.

   This displays a list of possible selections for the communications option. Active components will have a check in the checkboxes to their left.

6. Check **Dial Up Networking** at the top of the list and **Virtual Private Networking** at the bottom of the list.

7. Click **OK** at the bottom right on each screen until you return to the Control Panel. Close the Control Panel by clicking the upper right corner X.

8. Double-click the **My Computer** icon (normally at the left upper corner of the screen).

   This will display the devices within My Computer. Scroll down the list to **Dial-Up Networking** and double-click it.

9. Double click **Make New Connection**.

   This displays the Make New Connection installation screen. In this screen you will see a box labelled **Select a device**. From the pull-down menu to the right, select **Microsoft VPN Adapter**.

   Click the **Next** button at the bottom of the screen

   This displays the **VPN Host** screen. In the box to the top center of the screen enter your VPN server's IP address (for example, 192.168.xxx.xxx. This is not a proper Internet address)

Windows 98 VPN installation

1. From the Windows 98 **Start** menu select **Settings**, then **Control Panel** and click once.

   The Control Panel screen appears.

2. Double-click **Add/Remove Programs**.

   The Add/Remove Programs screen appears.

3. Click the **Windows Setup** tab.

   The Windows Setup screen will be displayed within the top center box.

4. Double-click **Communications**.

   This displays a list of possible selections for the communications option. Active components will have a check in the checkboxes to their left.

5. Check **Dial Up Networking** at the top of the list and **Virtual Private Networking** at the bottom of the list.

6. Click **OK** at the bottom right on each screen until you return to the Control Panel. Close the Control Panel by clicking the upper right corner X.

7. Double-click the **My Computer** icon (normally at the left upper corner of the screen).

   This will display the devices within My Computer. Scroll down the list to **Dial-Up Networking** and double-click it.

8. Double click **Make New Connection**.

   This displays the Make New Connection installation screen. In this screen you will see a box labelled **Select a device**. From the pull-down menu to the right, select **Microsoft VPN Adapter**.

   Click the **Next** button at the bottom of the screen

   This displays the **VPN Host** screen. In the box to the top center of the screen enter your VPN server's IP address (for example, 192.168.xxx.xxx. This is not a proper Internet address)

Connecting using Dial-Up Networking

A Dial-Up Networking connection will be automatically launched whenever you run a TCP/IP application, such as a web browser or email client. When you first run the application a Connect To dialog box appears in which you enter your User name and Password. If you check the Save password checkbox, the system will remember your User name and Password, and you won't be prompted for them again.

About ATMP Tunnels

To set up an ATMP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote ATMP partner. ATMP uses the terminology of a *foreign agent* that initiates tunnels and a *home agent* that terminates them. You use the same procedure to initiate or terminate an ATMP tunnel. Used in this way, the terms *initiate* and *terminate* mean the beginning and end of the tunnel; they do not mean *activate* and *deactivate*.

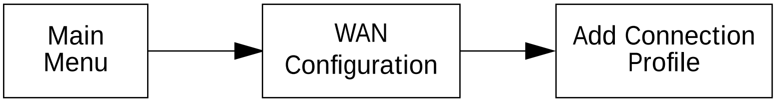
ATMP is a tunneling protocol, with two basic aspects. Tunnels are created and torn down using a session protocol that is UDP-based. User (or client) data is transferred across the tunnel by encapsulating the client data within Generic Routing Encapsulation (GRE). The GRE data is then routed using standard methods.

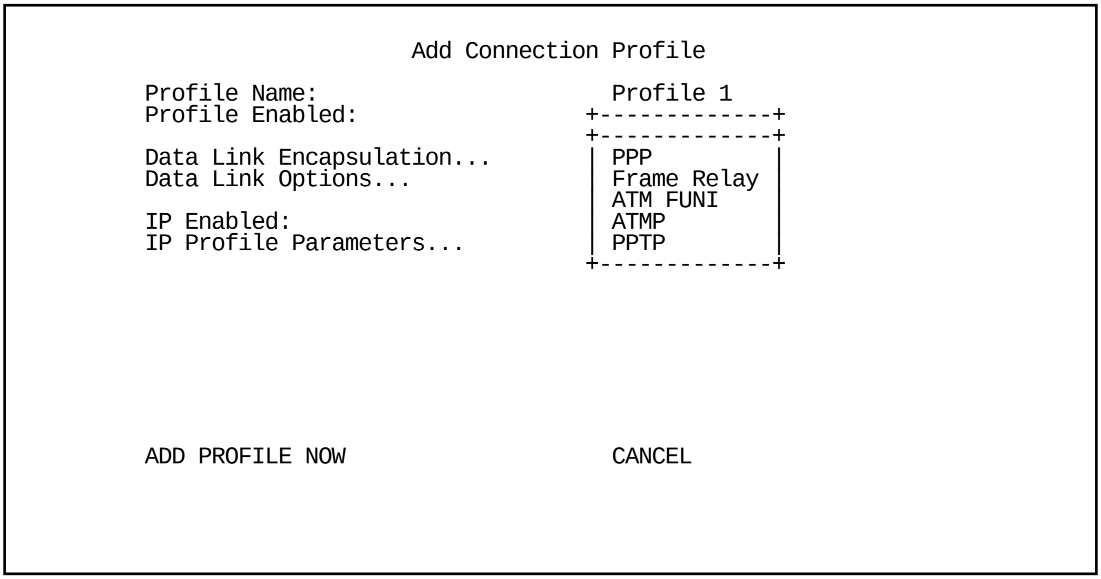
ATMP Configuration

ATMP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, since ATMP is not a native encapsulation. The Easy Setup Profile does not offer ATMP datalink encapsulation. See "Creating a new Connection Profile" on page 7-2 for information on creating Connection Profiles.

The WAN Event History screens will report VPN tunnel events, such as connections and disconnections, as Channel 4 (and higher) events.

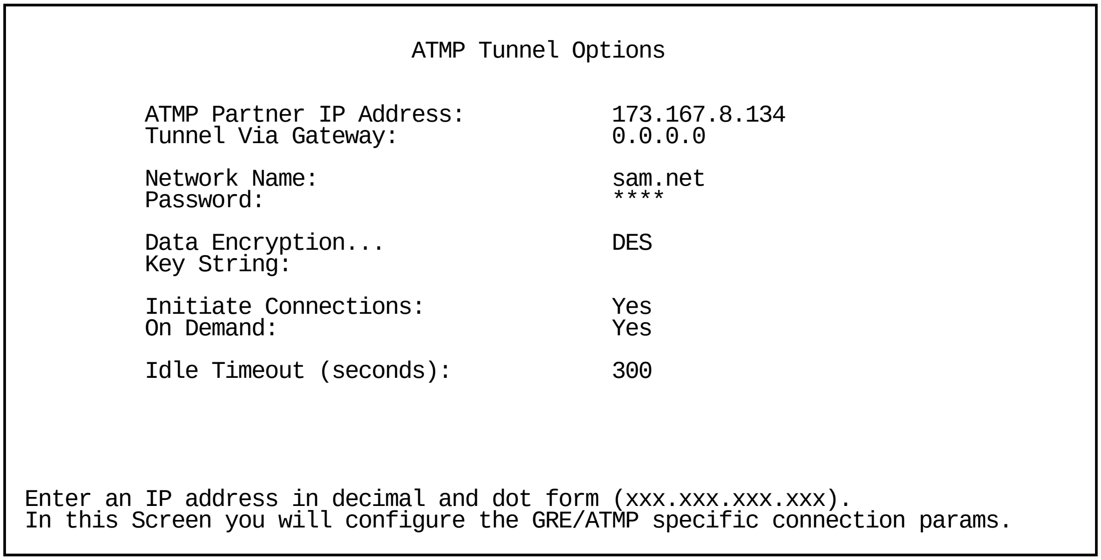
To define an ATMP tunnel, navigate to the **Add Connection Profile** menu from the Main Menu.





```
                          Add Connection Profile

  Profile Name:                      Profile 1
  Profile Enabled:                 +-------------+
                                   +-------------+
  Data Link Encapsulation...       | PPP         |
  Data Link Options...             | Frame Relay |
                                   | ATM FUNI    |
  IP Enabled:                      | ATMP        |
  IP Profile Parameters...         | PPTP        |
                                   +-------------+




  ADD PROFILE NOW                    CANCEL
```

When you define a Connection Profile as using ATMP by selecting ATMP as the datalink encapsulation method, and then select **Data Link Options**, the ATMP Tunnel Options screen appears.



```
                                 ATMP Tunnel Options

          ATMP Partner IP Address:           173.167.8.134
          Tunnel Via Gateway:                0.0.0.0

          Network Name:                      sam.net
          Password:                          ****

          Data Encryption...                 DES
          Key String:

          Initiate Connections:              Yes
          On Demand:                         Yes

          Idle Timeout (seconds):            300




 Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
 In this Screen you will configure the GRE/ATMP specific connection params.
```

Note: An ATMP tunnel cannot be assigned a dynamic IP address by the remote server, as in a PPP connection. When you define an ATMP tunnel profile, the Local WAN IP Address, assigned in the IP Profile Parameters screen, must be the true IP address, not 0.0.0.0, if NAT is enabled.

Note: Profiles using ATMP do not offer a Telco Options screen.

- **ATMP Partner IP Address** specifies the address of the other end of the tunnel. When unspecified, the gateway can not initiate tunnels (i.e., act as a foreign agent) for this profile; it can only accept tunnel requests as a home agent.

- When you specify the ATMP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, you can specify the route (**Tunnel Via Gateway**) by which the gateway partner is reached. If you do not specify the ATMP Partner IP Address, the router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e., the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.

- You can specify a **Network Name**. When the tunnel partner is another Netopia router, this name may be used to match against a Connection Profile. When the partner is an Ascend router in Gateway mode, then **Network Name** is used by the Ascend router to match a gateway profile. When the partner is an Ascend router in Router mode, leave this field blank.

- You must specify a **Password**, used for authenticating the tunnel.

  Note: The Password entry will be the same for both ends of the tunnel.

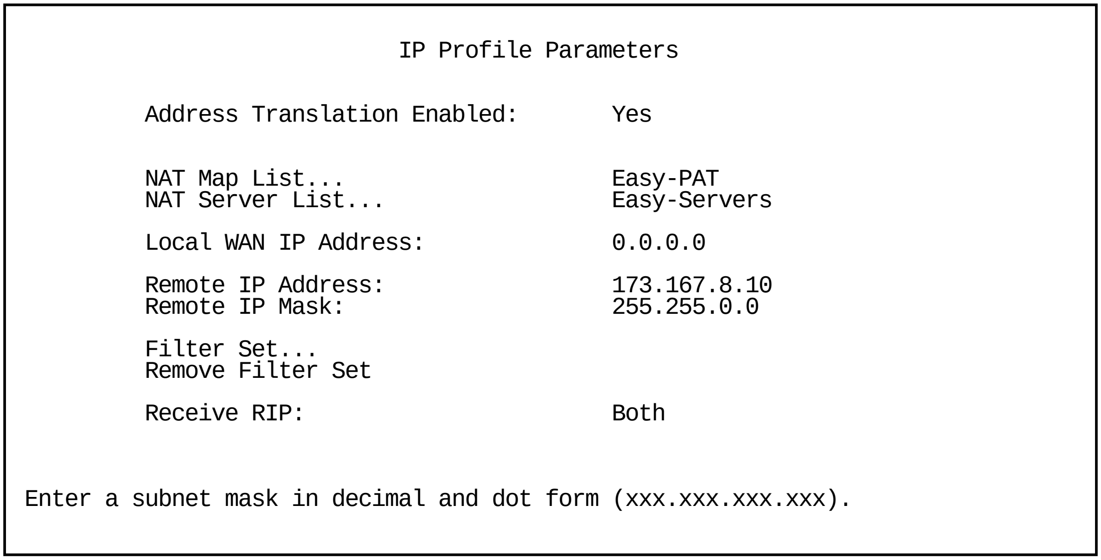
- For Netopia-to-Netopia connections only, you can specify a **Data Encryption** algorithm for the ATMP connection from the pop-up menu, either DES or None. None is the default.

  Note: Ascend does not support DES encryption for ATMP tunnels.

- You must specify an 8-byte **Key String** when DES is selected. When encryption is None, this field is invisible.

- You can specify that this router will **Initiate Connections**, acting as a foreign agent (**Yes**), or only answer them, acting as a home agent (**No**).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established through the call management screens.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.

  An alternate way to force a tunnel to stay up is to define a forced up scheduled connection for the profile. See "Scheduled connections" on page 8-7 for more information.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.



```
                        IP Profile Parameters

         Address Translation Enabled:       Yes


         NAT Map List...                    Easy-PAT
         NAT Server List...                 Easy-Servers

         Local WAN IP Address:              0.0.0.0

         Remote IP Address:                 173.167.8.10
         Remote IP Mask:                    255.255.0.0

         Filter Set...
         Remove Filter Set

         Receive RIP:                       Both


Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).
```

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

Note: A peculiarity associated with VPNs is that when a foreign agent has NAT applied to a Connection Profile set for ATMP data link encapsulation, the home agent and devices behind it, cannot Ping the foreign agent's tunnel end-point IP address. This is because ICMP packets have no port association, and thus will be discarded rather than being processed by NAT.

Ordinarily, Ping is an excellent troubleshooting tool, but it will not be effective in this circumstance. Instead, use another TCP- or UDP-based network service for troubleshooting. Since the Netopia Router is capable of serving Telnet and HTTP, we recommend using these services instead of Ping.

Allowing VPNs though a firewall

An administrator interested in securing a network will usually combine the use of VPNs with the use of a firewall or some similar mechanism. This is because a VPN is not a complete security solution, but rather a component of overall security. Using a VPN will add security to transactions carried over a public network, but a VPN alone will not prevent a public network from infiltrating a private network. Therefore, you should combine use of a firewall with VPNs, where the firewall will secure the private network from infiltration from a public network, and the VPN will secure the transactions that must cross the public network.

A strict firewall may not be provisioned to allow VPN traffic to pass back and forth as needed. In order to ensure that a firewall will allow a VPN, certain attributes must be added to the firewall's provisioning. The provisions necessary vary slightly between ATMP and PPTP, but both protocols operate on the same basic premise: there are control and negotiation operations, and there is the tunnelled traffic that carries the payload of data between the VPN endpoints. The difference is that ATMP uses UDP to handle control and negotiation, while PPTP uses TCP. Then both ATMP and PPTP use GRE to carry the payload.

For PPTP negotiation to work, TCP packets inbound and outbound destined for port 1723 must be allowed. Likewise, for ATMP negotiation to work, UDP packets inbound and outbound destined for port 5150 must be allowed. Source ports are dynamic, so, if possible, make this flexible, too. Additionally, PPTP and ATMP both require a firewall to allow GRE bi-directionally.

The following sections illustrate a sample filtering setup to allow either PPTP or ATMP traffic to cross a firewall:

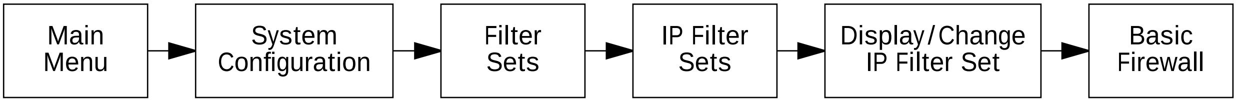
- "PPTP Example" on page 9-19
- "ATMP Example" on page 9-22

Make your own appropriate substitutions. For more information on filters and firewalls, see Chapter 14, "Security."

PPTP Example

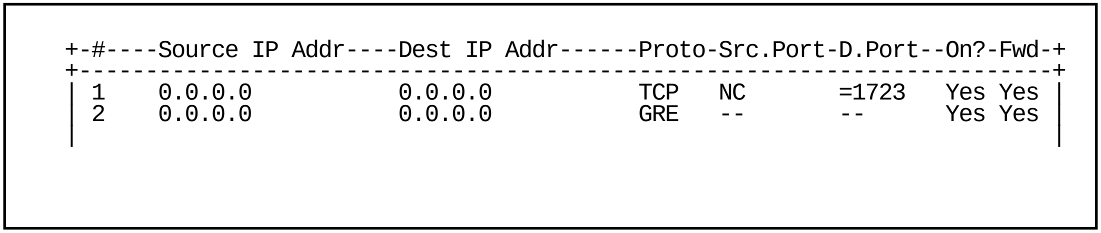
To enable a firewall to allow PPTP traffic, you must provision the firewall to allow inbound and outbound TCP packets specifically destined for port 1723. The source port may be dynamic, so often it is not useful to apply a compare function upon this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets, enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



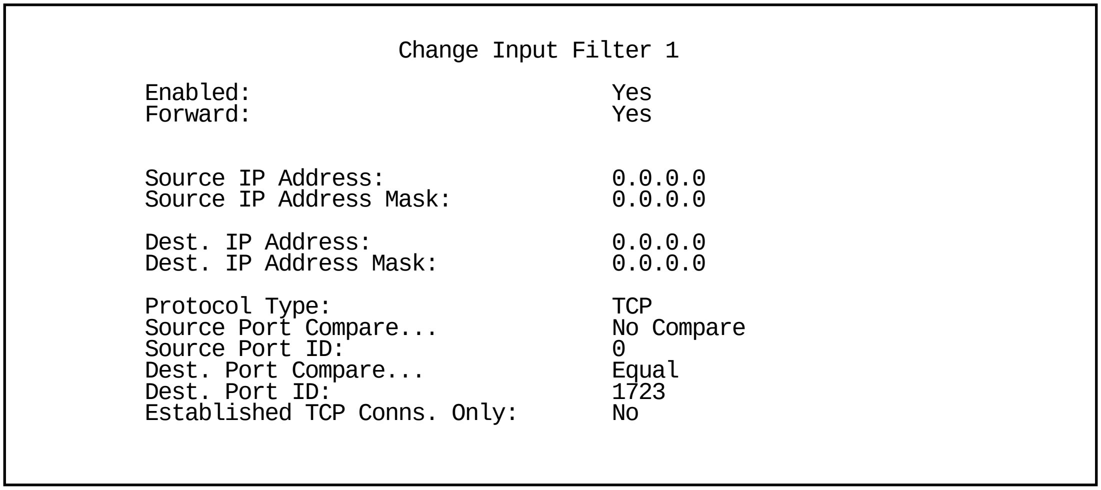
Select **Display / Change Input Filter**.

Display/Change Input Filter screen



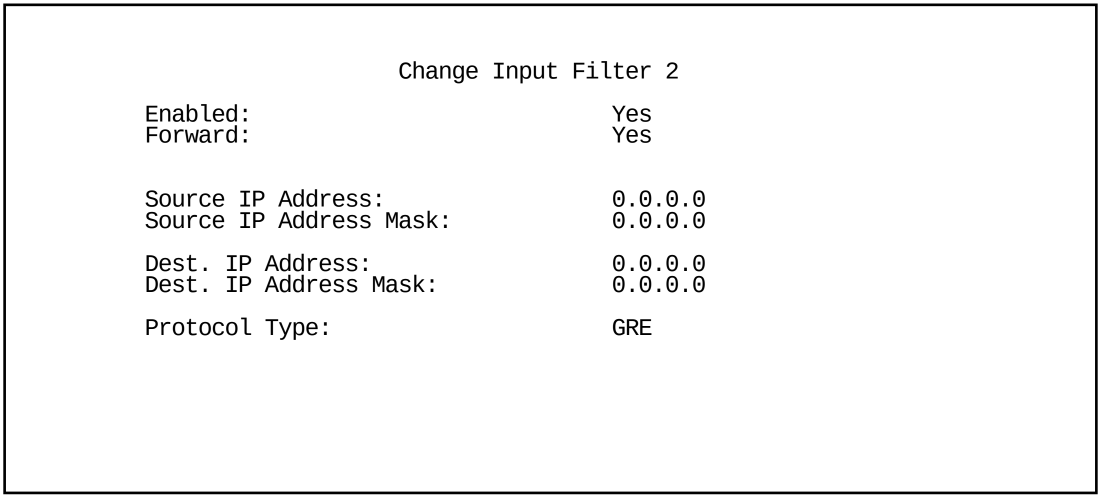
```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0           0.0.0.0           TCP   NC       =1723   Yes Yes |
| 2    0.0.0.0           0.0.0.0           GRE   --       --      Yes Yes |
|                                                                         |
```

For Input Filter 1 set the Destination Port information as shown below.



```
                         Change Input Filter 1

      Enabled:                           Yes
      Forward:                           Yes


      Source IP Address:                 0.0.0.0
      Source IP Address Mask:            0.0.0.0

      Dest. IP Address:                  0.0.0.0
      Dest. IP Address Mask:             0.0.0.0

      Protocol Type:                     TCP
      Source Port Compare...             No Compare
      Source Port ID:                    0
      Dest. Port Compare...              Equal
      Dest. Port ID:                     1723
      Established TCP Conns. Only:       No
```

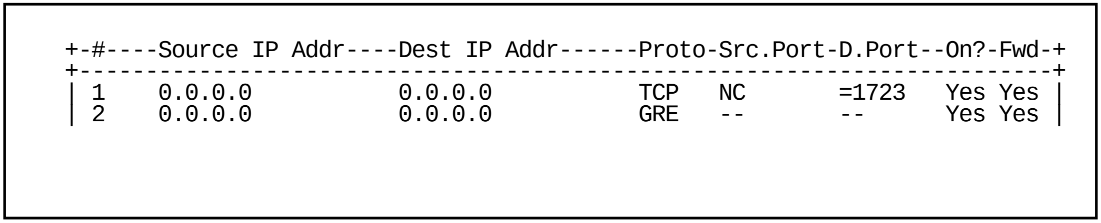
For Input Filter 2 set the Protocol Type to allow GRE as shown below.



```
                         Change Input Filter 2

      Enabled:                           Yes
      Forward:                           Yes


      Source IP Address:                 0.0.0.0
      Source IP Address Mask:            0.0.0.0

      Dest. IP Address:                  0.0.0.0
      Dest. IP Address Mask:             0.0.0.0

      Protocol Type:                     GRE
```

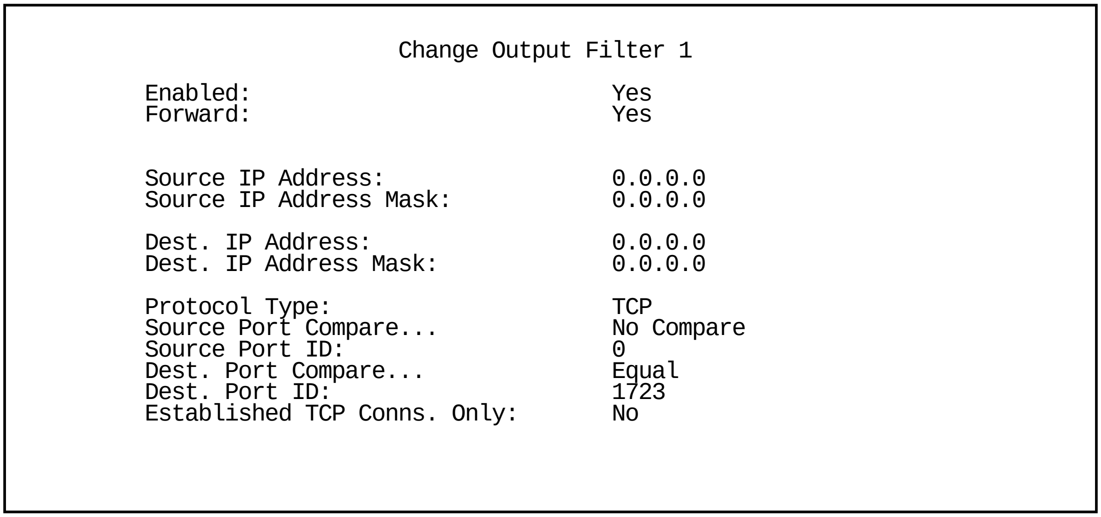
In the Display/Change IP Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen



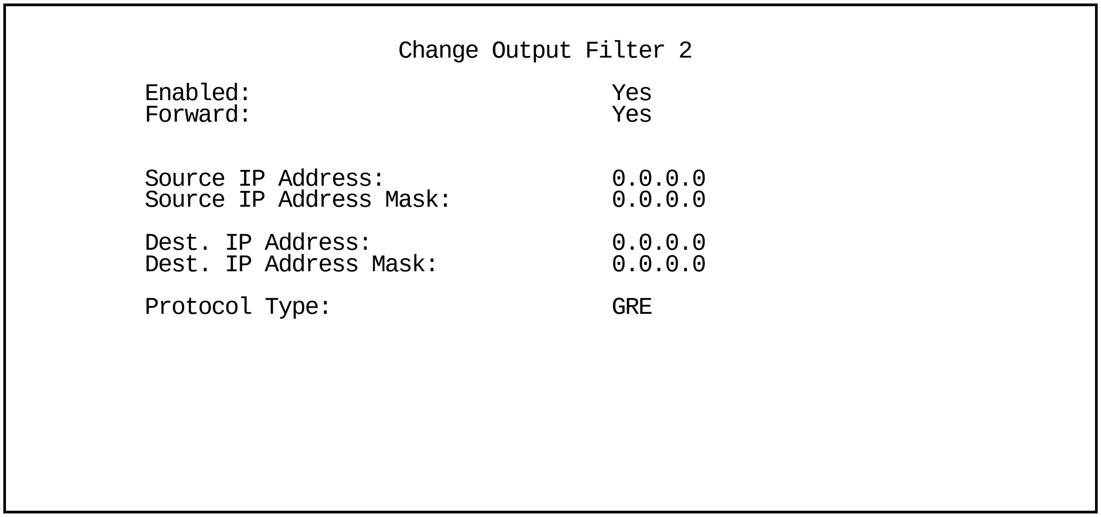
```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0          0.0.0.0          TCP   NC       =1723   Yes Yes |
| 2    0.0.0.0          0.0.0.0          GRE   --       --      Yes Yes |
```

For Output Filter 1 set the Protocol Type and Destination Port information as shown below.



```
                       Change Output Filter 1

      Enabled:                          Yes
      Forward:                          Yes


      Source IP Address:                0.0.0.0
      Source IP Address Mask:           0.0.0.0

      Dest. IP Address:                 0.0.0.0
      Dest. IP Address Mask:            0.0.0.0

      Protocol Type:                    TCP
      Source Port Compare...            No Compare
      Source Port ID:                   0
      Dest. Port Compare...             Equal
      Dest. Port ID:                    1723
      Established TCP Conns. Only:      No
```

For Output Filter 2 set the Protocol Type to allow GRE as shown below.

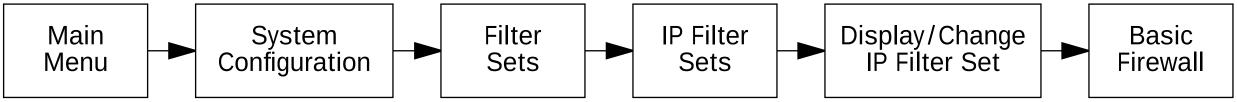


```
                       Change Output Filter 2

      Enabled:                          Yes
      Forward:                          Yes


      Source IP Address:                0.0.0.0
      Source IP Address Mask:           0.0.0.0

      Dest. IP Address:                 0.0.0.0
      Dest. IP Address Mask:            0.0.0.0

      Protocol Type:                    GRE
```

ATMP Example

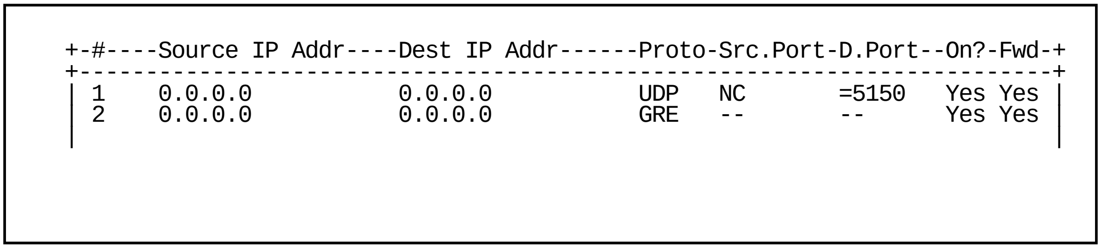
To enable a firewall to allow ATMP traffic, you must provision the firewall to allow inbound and outbound UDP packets specifically destined for port 5150. The source port may be dynamic, so often it is not useful to apply a compare function on this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets (Protocol 47, Internet Assigned Numbers Document, RFC 1700), enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



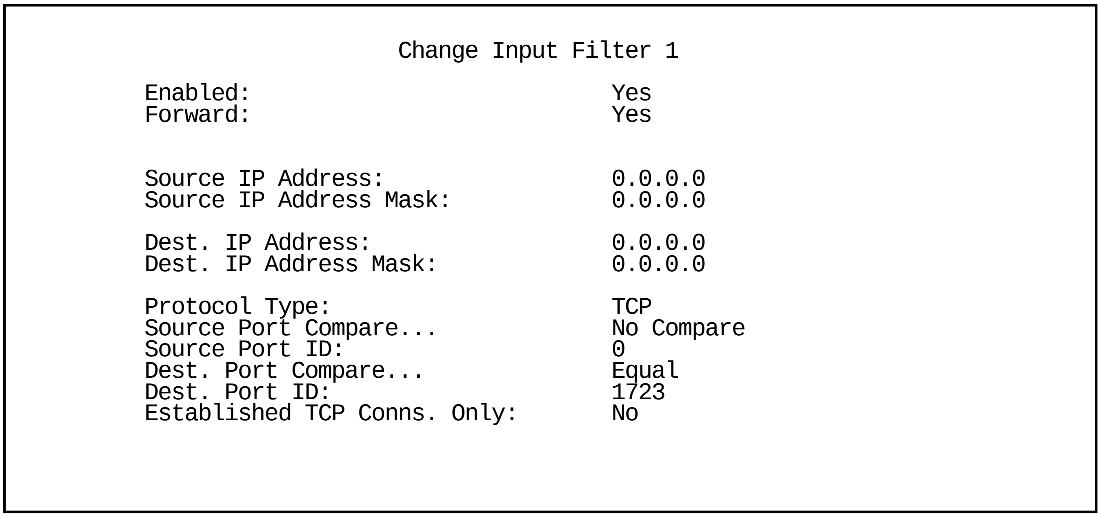
Select **Display/Change Input Filter**.

Display/Change Input Filter screen



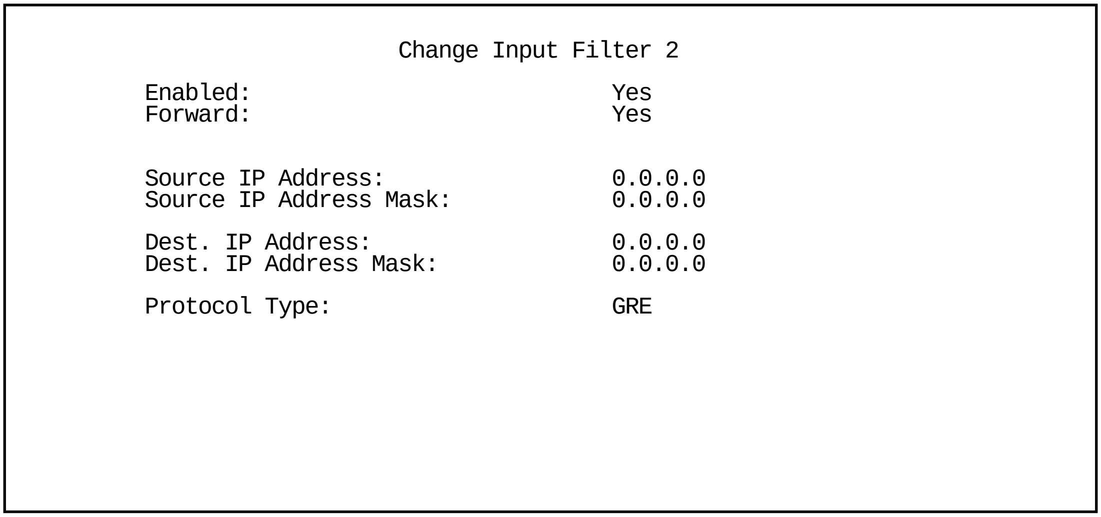
```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0           0.0.0.0           UDP   NC       =5150   Yes Yes |
| 2    0.0.0.0           0.0.0.0           GRE   --       --      Yes Yes |
|                                                                         |
```

For Input Filter 1 set the Destination Port information as shown below.



```
                        Change Input Filter 1

      Enabled:                          Yes
      Forward:                          Yes


      Source IP Address:                0.0.0.0
      Source IP Address Mask:           0.0.0.0

      Dest. IP Address:                 0.0.0.0
      Dest. IP Address Mask:            0.0.0.0

      Protocol Type:                    TCP
      Source Port Compare...            No Compare
      Source Port ID:                   0
      Dest. Port Compare...             Equal
      Dest. Port ID:                    1723
      Established TCP Conns. Only:      No
```

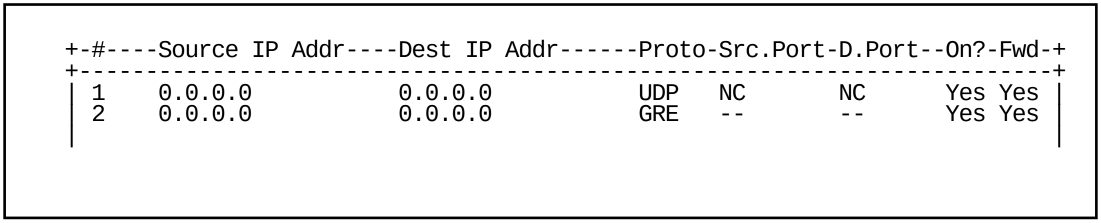
For Input Filter 2 set the Protocol Type to allow GRE as shown below.



```
                    Change Input Filter 2

     Enabled:                          Yes
     Forward:                          Yes


     Source IP Address:                0.0.0.0
     Source IP Address Mask:           0.0.0.0

     Dest. IP Address:                 0.0.0.0
     Dest. IP Address Mask:            0.0.0.0

     Protocol Type:                    GRE
```

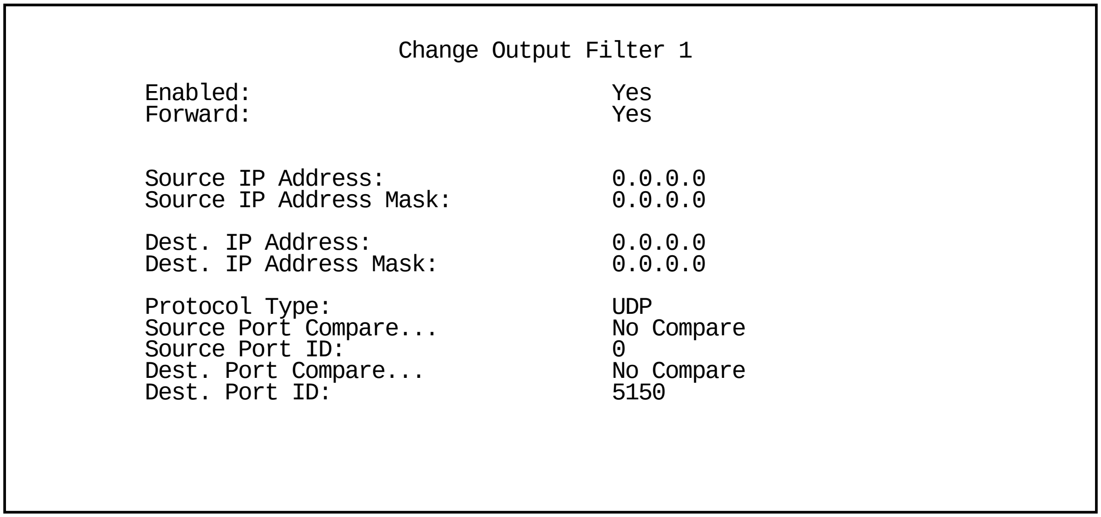
In the Display/Change IP Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen



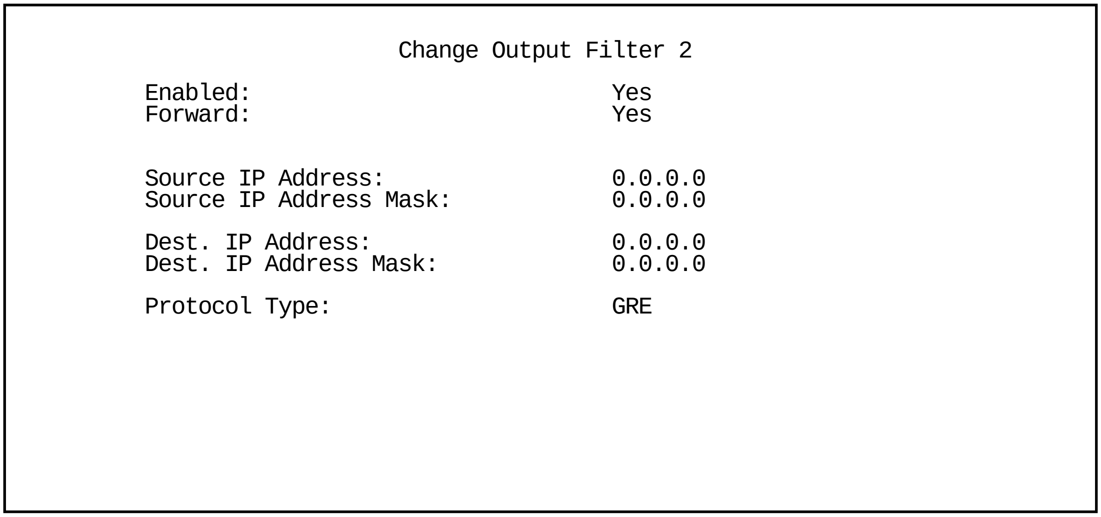
```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0           0.0.0.0           UDP   NC       NC      Yes Yes |
| 2    0.0.0.0           0.0.0.0           GRE   --       --      Yes Yes |
|                                                                         |
```

For Output Filter 1 set the Protocol Type and Destination Port information as shown below.



```
                    Change Output Filter 1

     Enabled:                          Yes
     Forward:                          Yes


     Source IP Address:                0.0.0.0
     Source IP Address Mask:           0.0.0.0

     Dest. IP Address:                 0.0.0.0
     Dest. IP Address Mask:            0.0.0.0

     Protocol Type:                    UDP
     Source Port Compare...            No Compare
     Source Port ID:                   0
     Dest. Port Compare...             No Compare
     Dest. Port ID:                    5150
```

For Output Filter 2 set the Protocol Type to allow GRE as shown below.



```
                    Change Output Filter 2

     Enabled:                           Yes
     Forward:                           Yes


     Source IP Address:                 0.0.0.0
     Source IP Address Mask:            0.0.0.0

     Dest. IP Address:                  0.0.0.0
     Dest. IP Address Mask:             0.0.0.0

     Protocol Type:                     GRE
```

Chapter 10

Multiple Network Address Translation and IP Setup

The Netopia R2020 uses Internet Protocol (IP) to communicate both locally and with remote networks. This chapter shows you how to configure the Router to route IP traffic. You also learn how to configure the Router to serve IP addresses to hosts on your local network.

Netopia's SmartIP features IP address serving and Network Address Translation. This chapter describes how to use the Network Address Translation feature of SmartIP and Multiple Network Address Translation (MultiNAT).

Note: When you configured your Netopia R2020 using SmartStart, Network Address Translation was enabled by default. You have the option of disabling it, if you wish. This is done through the System Configuration screens using Console-based Management.

This section covers the following topics:

Overview

NAT (Network Address Translation) is a means whereby one or more IP addresses and/or IP service ports are re-mapped into other values. This *aliasing* serves two functions:

- It allows the addresses of many computers to be represented by only one or a few addresses, saving you money.
- It can be used as a security feature by obscuring the true addresses of important machines from potential hackers on the Internet.

To help you understand some of the concepts discussed here, it may be helpful to introduce some NAT terminology.

The terms *mapping* or *remapping* refer to rules that translate one or more addresses on the Netopia Router's LAN to another address or addresses on the other side of the Netopia Router's WAN link (typically the Internet).

The terms *private* and *internal* refer to addresses on the Netopia Router's LAN network that are protected or obscured from the NAT remappings. These *NATed* addresses cannot be seen from the Internet side of the Netopia Router's WAN connection.

The terms *public* and *external* refer to the Internet side of the Netopia Router's connection. A machine on the public network cannot necessarily access a machine behind a Netopia Router's NAT remapping, unless you specify that it can.

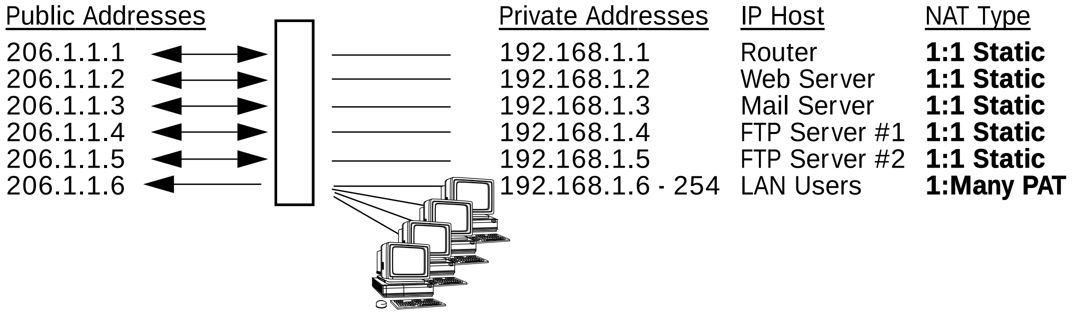
Multiple Network Address Translation (MultiNAT) introduces several new NAT-related features. These features can be divided into three categories that can be used simultaneously in different combinations on a per-Connection Profile basis.

A brief description follows:

- *PAT* stands for Port Address Translation (also known as NAPT for Network Address Port Translation). It allows an entire network or part of a network to be represented to the outside world as a single IP address. A limitation of PAT is that communication must be initiated from the internal network. A user on the external side can not access a machine behind a PAT connection. Now, with the Netopia R2020 Router, you can define multiple PAT remappings. Each of these can optionally alias a section or *range* of IP addresses of the internal network. PAT remapping allows only internal users to initiate traffic flow between the internal and external networks.
- *Static remappings* are a way to represent an internal single address or sequence of addresses as an external address or sequence of addresses on a one-to-one basis. As with PAT remappings, you can simultaneously use several static rules. Machines on the external network can initiate conversations with statically remapped internal computers by accessing the aliased values. It is important to note that in most uses of static remappings a static route on the external router must be created to tell the external network to go through the NAT Netopia Router to get to the remapped external addresses. Static remapping allows an entire machine to be available to the external net. Either the internal NATed machine or the external network can initiate traffic flow to or from the remapped machine.
- *Server Lists* are also known as *exported services*. By creating a server list, you can tell the outside world that specific *services* such as Web, ftp, e-mail, etc. can be accessed at specific external addresses. Server lists differ from static remappings in that the specified service is only available to external users at the stated alias address. In most uses of server lists you must create a static route on the external router to tell the external network to go through the NAT Netopia Router to get to the remapped address of the server lists. Exported servers and Server Lists allow only specific IP services (IP ports) to be available to the outside world. Services from different internal machines can be presented as a single external IP address.

Map Lists and Server Lists are completely independent of each other. A Connection Profile can use one or the other or both.

MultiNAT allows complex mapping and requires some complex configuration. Multiple mapped interior subnets are supported, and the rules for mapping each of the subnets may be different. The figure below illustrates a possible multiNAT configuration.



Public Addresses	Private Addresses	IP Host	NAT Type
206.1.1.1	192.168.1.1	Router	**1:1 Static**
206.1.1.2	192.168.1.2	Web Server	**1:1 Static**
206.1.1.3	192.168.1.3	Mail Server	**1:1 Static**
206.1.1.4	192.168.1.4	FTP Server #1	**1:1 Static**
206.1.1.5	192.168.1.5	FTP Server #2	**1:1 Static**
206.1.1.6	192.168.1.6 - 254	LAN Users	**1:Many PAT**

In order to support this type of mapping, the private addresses and public addresses are separated and are assigned to ranges. Each range consists of a contiguous set of one or more addresses. The router allocates the addresses in that range based on the type (static or PAT), and other relevant attributes. The range defines the rules for distributing the exterior addresses. NAT maps, kept in a list similar to a firewall or filter list, contain the private addresses and the name pointer of the range to use to get a public address. The maps function as an access control list to the resource contained in the range.

Features

The Netopia R2020 Router features the following:

- Default behavior consistent with previous firmware versions, including PAT to a DHCP- or PPP-assigned address.
- 1-to-1 static NAT mapping.

  An internal private address is permanently mapped to an external address. TCP and UDP port addresses are not altered.
- Multiple Many-to-1 PAT mappings on a single interface.

  PAT addresses may be assigned to specific private address subnets; not all internal machines need to be included on a PAT remapping list.
- Coexistent mapped and unmapped traffic on a public interface.

  If the router's IP address is not included in a NAT list, it will be invisible to the external network.
- Mapped services (exports) may use multiple public addresses.
- NAT maps per interface, similar to the filter rules.

Supported traffic

MultiNat supports the following IP protocols:

- PAT: TCP/UDP traffic which does not carry source or destination IP addresses or ports in the data stream (i.e., HTTP, telnet, ‘r’ commands, tftp, NFS, NTP, SMTP, NNTP, etc.).
- Static NAT: All IP protocol traffic which does not carry or otherwise rely on the source or destination IP addresses in the data stream.

NAT configuration

You use the NAT feature sets by defining a series of remapping rules and then grouping them into a *list*. There are two kinds of lists -- *Map Lists*, made up of PAT and Static remapping rules, and *Server Lists*, a list of internal services to be presented to the external world. Creating these lists is a four-step process:

1. **Define the public range** of addresses that external computers should use to get to the NAT internal machines. These are the addresses that someone on the Internet would see.
2. **Create a List name** that will act as a rule or server holder.
3. **Create an internal *map*** or rule that specifies the internal range of NATed addresses and how they are to be aliased to the external range.
4. **Associate the Map or Server List to your WAN interface** via a Connection Profile or the Default Profile.

The three NAT features all operate completely independently of each other, although they can be used simultaneously on the same Connection Profile.

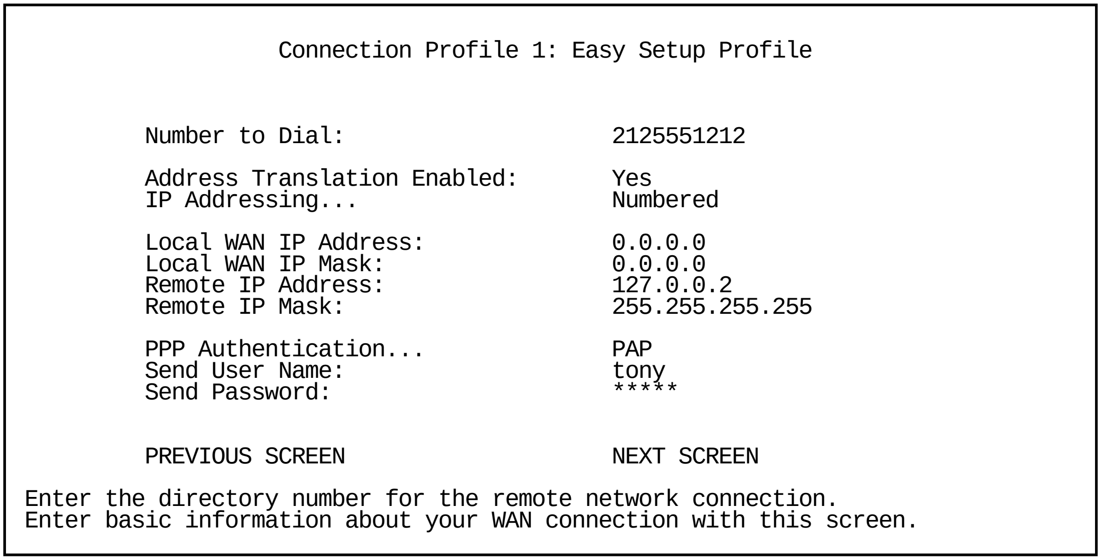
You can configure a simple 1-to-many PAT (often referred to simply as NAT) mapping using Easy Setup. More complex setups require configuration using the **Network Address Translation** item on the IP Setup screen.

An example MultiNAT configuration at the end of this chapter describes some applications for these features. See "MultiNAT Configuration Example" on page 10-24.

You configure the MultiNAT features through the console menu in three areas:

- Easy Setup Profile, described on page 10-4.
- IP setup, described on page 10-5.
- IP profile parameters, described on page 10-18.

Easy Setup Profile



```
                    Connection Profile 1: Easy Setup Profile


         Number to Dial:                  2125551212

         Address Translation Enabled:     Yes
         IP Addressing...                 Numbered

         Local WAN IP Address:            0.0.0.0
         Local WAN IP Mask:               0.0.0.0
         Remote IP Address:               127.0.0.2
         Remote IP Mask:                  255.255.255.255

         PPP Authentication...            PAP
         Send User Name:                  tony
         Send Password:                   *****


         PREVIOUS SCREEN                  NEXT SCREEN

Enter the directory number for the remote network connection.
Enter basic information about your WAN connection with this screen.
```

- The **Local WAN IP Address** is used to configure a NAT public address range consisting of the Local WAN IP Address and all its ports. The public address map list is named *Easy-PAT List* and the port map list is named *Easy-Servers*.

  When you exit this screen the two map lists, Easy-PAT List and Easy-Servers, are created by default and NAT configuration becomes effective.This will map all your private addresses (0.0.0.0 through 255.255.255.255) to your public address. These map lists are bound to the Easy Setup Profile. See "Binding Map Lists and Server Lists" on page 10-18.

  This is all you need to do if you want to continue to use a single PAT, or 1-to-many, NAT configuration.

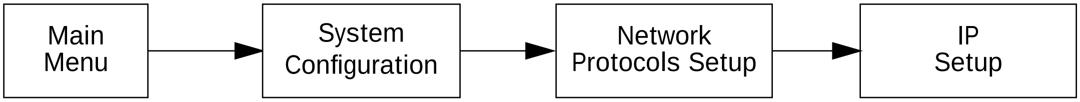
- In order to configure the router to make servers on your LAN visible to the Internet, you use advanced features in the System Configuration screens, described in "IP setup" on page 10-5.

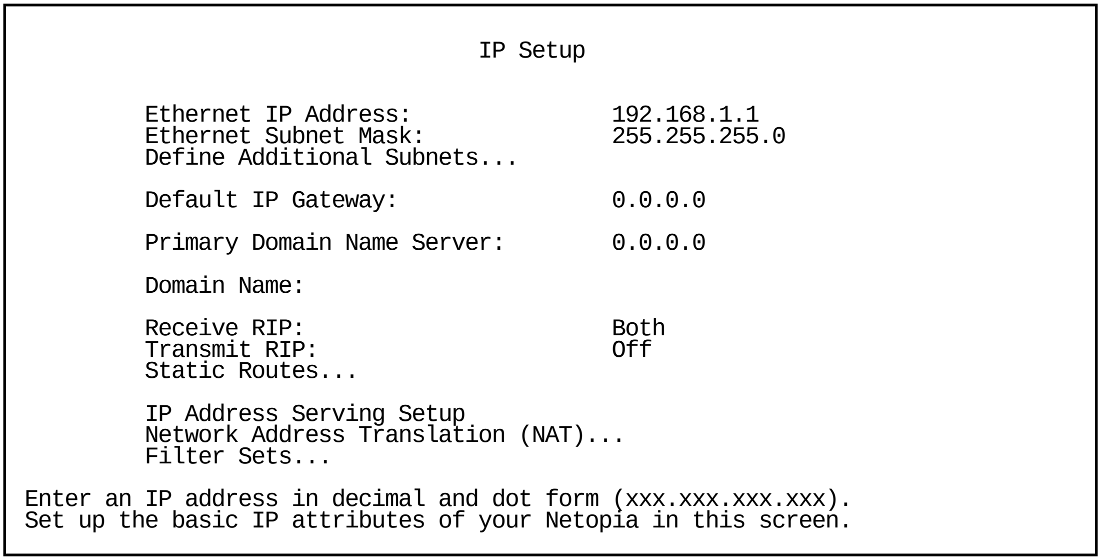
Note: There is no implicit binding between the WAN IP interface address and NAT, as in earlier firmware versions, so you cannot disallow configuration of NAT simply because the interface is numbered or disallow configuration of the addressing type (numbered or unnumbered) simply because NAT is enabled.

If the router has a numbered interface, then it is addressable by the IP address. With PAT, when NAT was enabled the interface would be marked unnumbered and the IP address subsumed by NAT. However, NAT would allow traffic directed to that IP address to be delivered to the router. This effectively made the interface a numbered interface. MultiNAT adds the option of true unnumbered NAT. Traffic delivered to the router on an unnumbered interface which cannot be processed by NAT is dropped.

IP setup

To access the NAT configuration screens, from the Main Menu navigate to IP Setup:

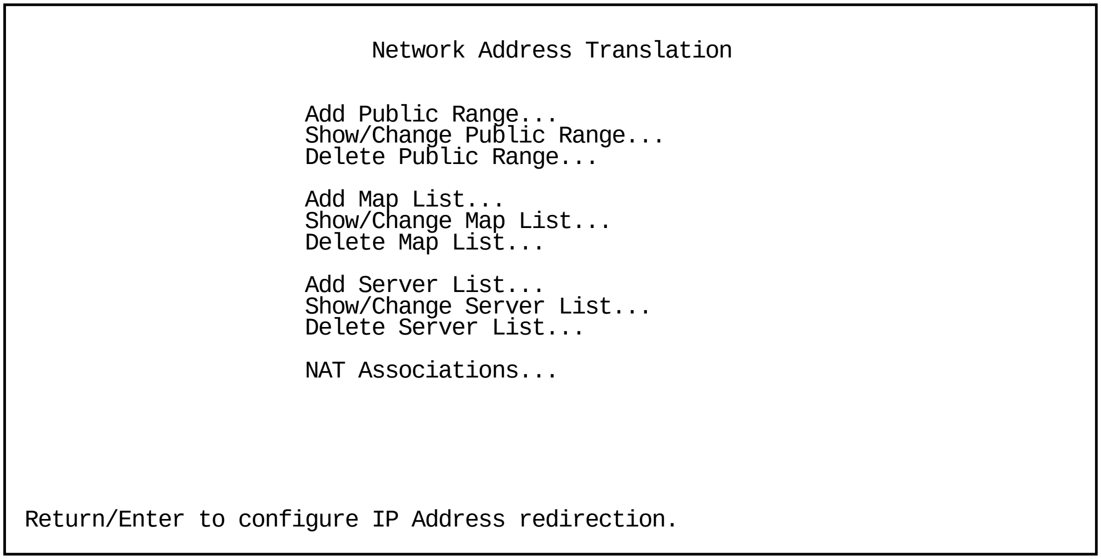




```
                              IP Setup


         Ethernet IP Address:                  192.168.1.1
         Ethernet Subnet Mask:                 255.255.255.0
         Define Additional Subnets...

         Default IP Gateway:                   0.0.0.0

         Primary Domain Name Server:           0.0.0.0

         Domain Name:

         Receive RIP:                          Both
         Transmit RIP:                         Off
         Static Routes...

         IP Address Serving Setup
         Network Address Translation (NAT)...
         Filter Sets...

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
Set up the basic IP attributes of your Netopia in this screen.
```

Select **Network Address Translation (NAT)** and press Return.

The Network Address Translation screen appears.



```
                          Network Address Translation


                     Add Public Range...
                     Show/Change Public Range...
                     Delete Public Range...

                     Add Map List...
                     Show/Change Map List...
                     Delete Map List...

                     Add Server List...
                     Show/Change Server List...
                     Delete Server List...

                     NAT Associations...





Return/Enter to configure IP Address redirection.
```

Public Range: defines an external address range and indicates what type of remapping to apply when using this range. The types of remapping available are *static* and *pat*.

Map Lists: define collections of mapping rules. A rule maps interior range addresses to exterior range addresses by the mapping techniques defined in the map list.

Server Lists: bind internal IP addresses and ports to external IP addresses and ports so that connections initiated from the outside can access an interior server.

NAT rules

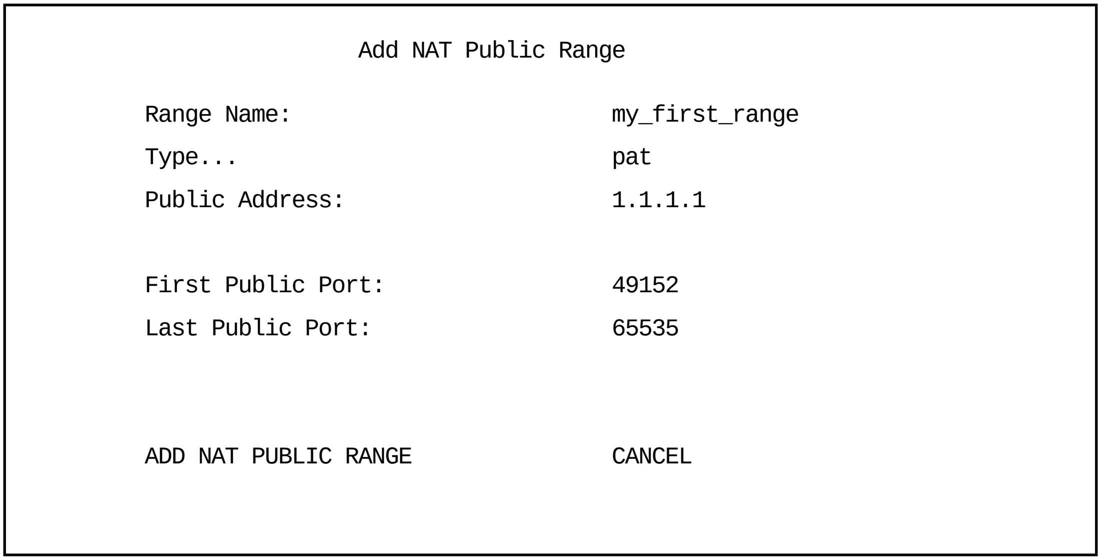
The following rules apply to assigning NAT ranges and server lists:

- Static public address ranges must not overlap other static, PAT, public addresses or the public address assigned to the router's WAN interface.
- A PAT public address must not overlap any static address ranges. It may be the same as another PAT address or server list address, but the port range must not overlap.

You configure the ranges of exterior addresses by first adding public ranges.

Select **Add Public Range** and press Return.

The Add NAT Public Range screen appears.



```
                          Add NAT Public Range

          Range Name:                         my_first_range
          Type...                             pat
          Public Address:                     1.1.1.1

          First Public Port:                  49152
          Last Public Port:                   65535



          ADD NAT PUBLIC RANGE                CANCEL
```

- Select **Range Name** and give a descriptive name to this range.
- Select **Type** and from the pop-up menu, assign its type. Options are static or pat (the default).
  - If you choose *pat* as the range type, select **Public Address** and enter the exterior IP address in the range you want to assign. Select **First** and **Last Public Port** and enter the first and last exterior ports in the range. These are the ports that will be used for traffic initiated from the private LAN to the outside world.

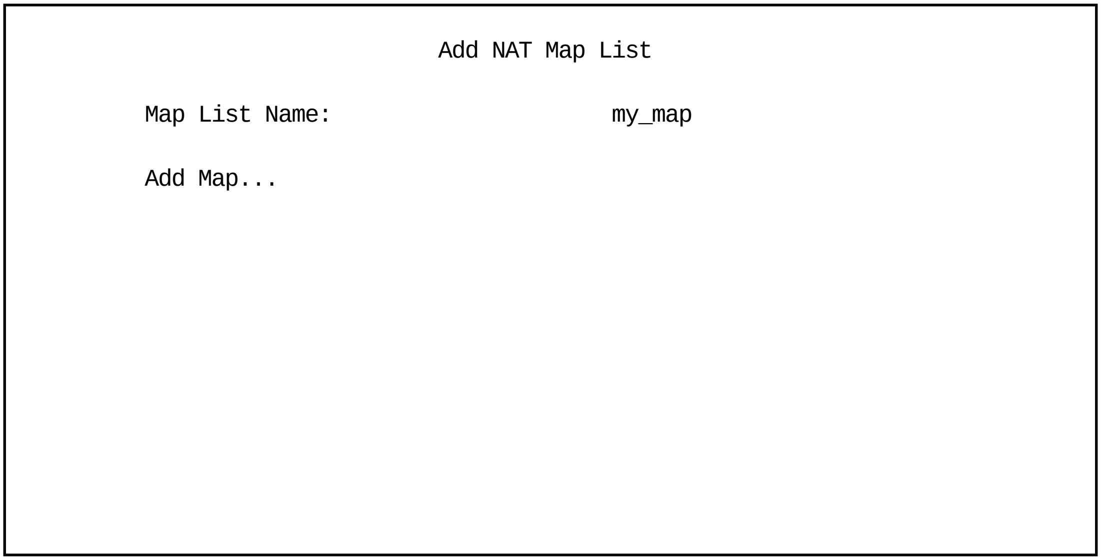
    Note: For PAT Map lists and Server lists, if you use the Public Address 0.0.0.0, the list will acquire its public IP address from the WAN IP address specified by your WAN IP configuration in the Connection Profile. If that is a static IP address, then the PAT map list and Server lists will acquire that address. If it is a negotiated IP address, such as may be assigned via DHCP or PPP, the PAT map list and Server lists will acquire that address each time it is negotiated.
  - If you choose *static* as the range type, a new menu item, **First Public Address**, becomes visible. Select **First Public Address** and enter the first exterior IP address in the range you want to assign. Select **Last Public Address** and enter an IP address at the end of the range.

- Select **ADD NAT PUBLIC RANGE** and press Return. The range will be added to your list and you will be returned to the Network Address Translation screen.

Once the public ranges have been assigned, the next step is to bind interior addresses to them. Because these bindings occur in ordered lists, called *map lists*, you must first define the list, then add mappings to it.

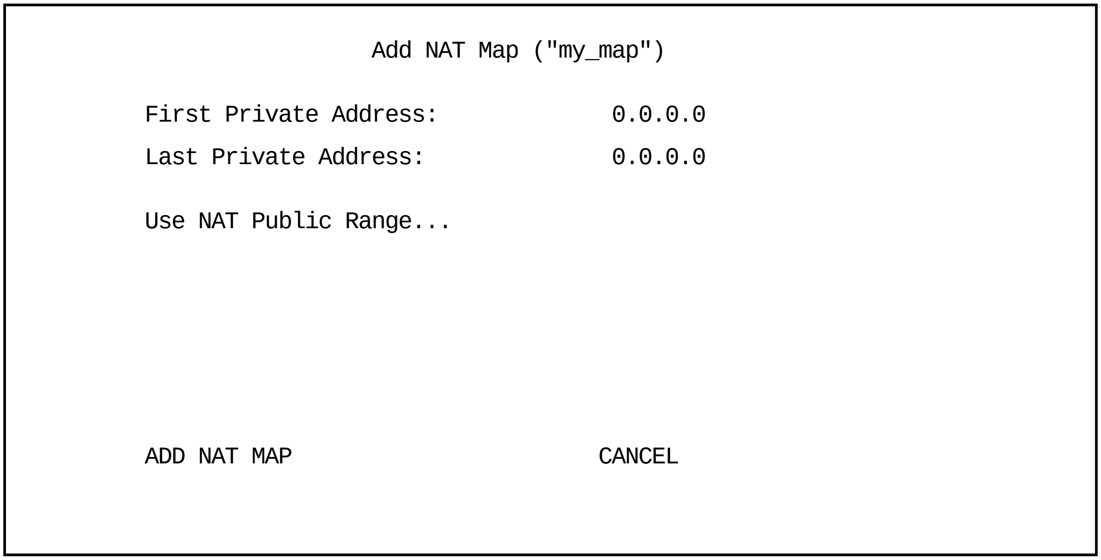
From the Network Address Translation screen select **Add Map List** and press Return.

The Add NAT Map List screen appears.



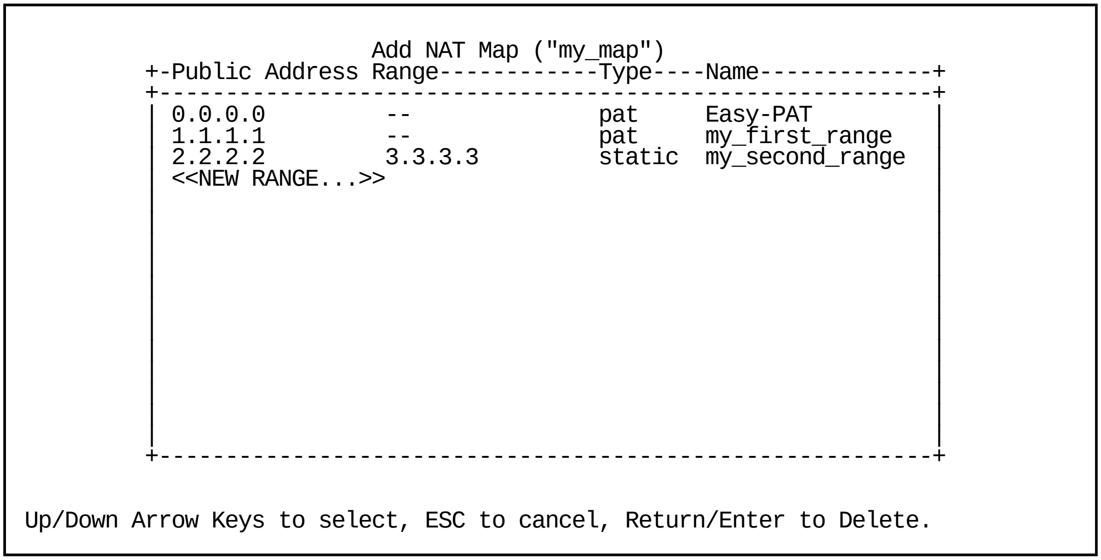
```
                              Add NAT Map List

          Map List Name:                     my_map

          Add Map...
```

- Select **Map List Name** and enter a descriptive name for this map list. A new menu item **Add Map** appears.
- Select **Add Map** and press Return. The Add NAT Map screen appears.



```
                         Add NAT Map ("my_map")

          First Private Address:             0.0.0.0
          Last Private Address:              0.0.0.0

          Use NAT Public Range...



          ADD NAT MAP                       CANCEL
```

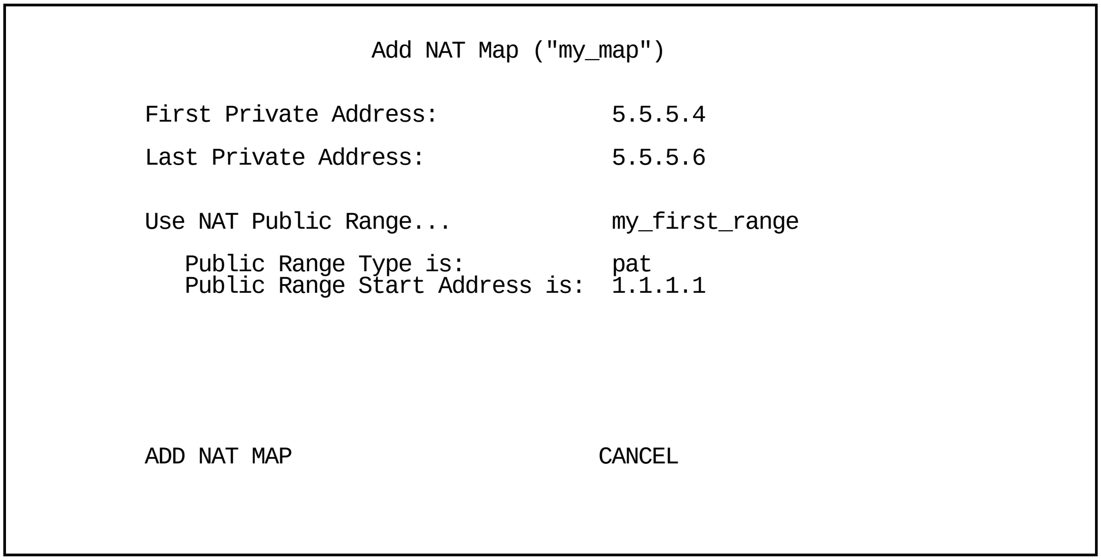
- Select **First** and **Last Private Address** and enter the first and last interior IP addresses you want to assign to this mapping.
- Select **Use NAT Public Range** and press Return. A screen appears displaying the public ranges you have defined.



```
                         Add NAT Map ("my_map")
            +-Public Address Range------------Type----Name-------------+
            +----------------------------------------------------------+
            | 0.0.0.0         --              pat     Easy-PAT          |
            | 1.1.1.1         --              pat     my_first_range    |
            | 2.2.2.2         3.3.3.3         static  my_second_range   |
            | <<NEW RANGE...>>                                          |
            |                                                           |
            |                                                           |
            |                                                           |
            |                                                           |
            |                                                           |
            |                                                           |
            |                                                           |
            |                                                           |
            |                                                           |
            |                                                           |
            |                                                           |
            |                                                           |
            |                                                           |
            +----------------------------------------------------------+


Up/Down Arrow Keys to select, ESC to cancel, Return/Enter to Delete.
```

- From the list of public ranges you defined, select the one that you want to map to the interior range for this mapping and press Return.

  If none of your preconfigured ranges are suitable for this mapping, you can select **<<NEW RANGE>>** and create a new range. If you choose **<<NEW RANGE>>**, the Add NAT Public Range screen displays and you can create a new public range to be used by this map. See "Add NAT Public Range" on page 10-7.
- The Add NAT Map screen now displays the range you have assigned.



```
                          Add NAT Map ("my_map")

         First Private Address:              5.5.5.4

         Last Private Address:               5.5.5.6

         Use NAT Public Range...             my_first_range

            Public Range Type is:            pat
            Public Range Start Address is:   1.1.1.1





         ADD NAT MAP                        CANCEL
```

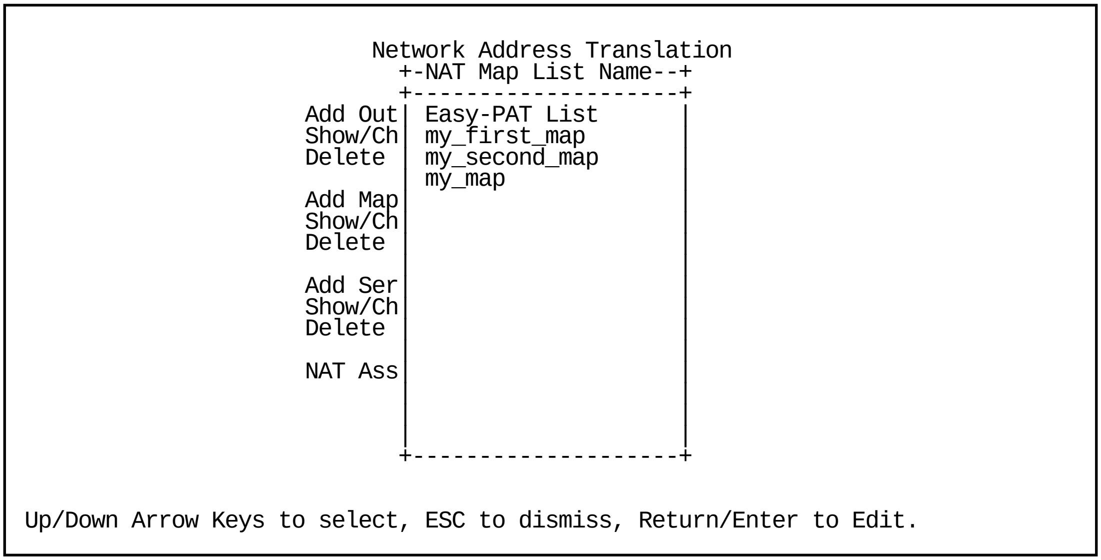
- Select **ADD NAT MAP** and press Return. Your mapping is added to your map list.

Modifying map lists

You can make changes to an existing map list after you have created it. Since there may be more than one map list you must select which one you are modifying.

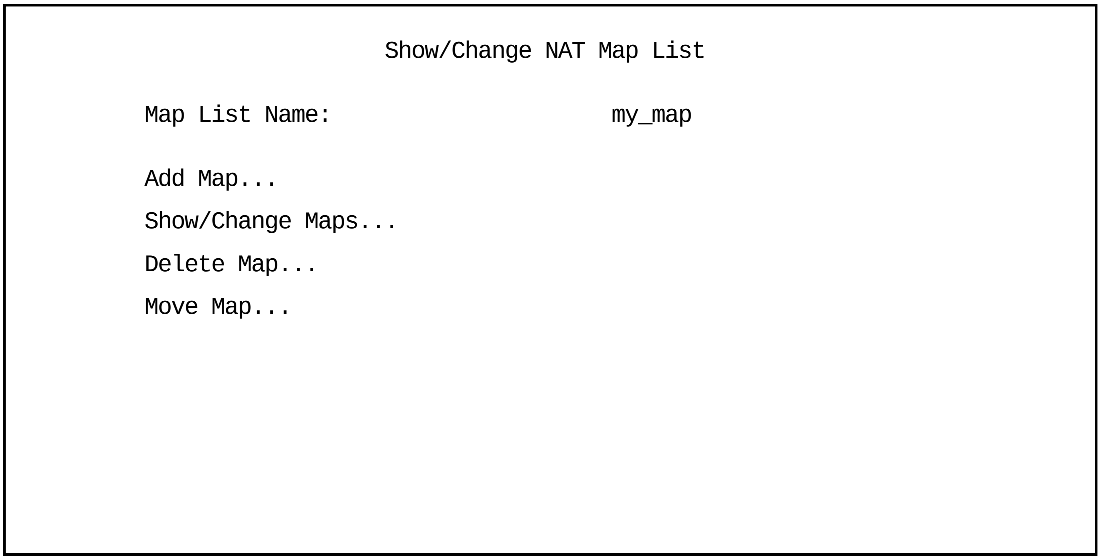
From the Network Address Translation screen select **Show/Change Map List** and press Return.

- Select the map list you want to modify from the popup menu.



```
                          Network Address Translation
                            +-NAT Map List Name--+
                            +--------------------+
                     Add Out|  Easy-PAT List     |
                     Show/Ch|  my_first_map      |
                     Delete |  my_second_map     |
                            |  my_map            |
                     Add Map|                    |
                     Show/Ch|                    |
                     Delete |                    |
                            |                    |
                     Add Ser|                    |
                     Show/Ch|                    |
                     Delete |                    |
                            |                    |
                     NAT Ass|                    |
                            |                    |
                            |                    |
                            +--------------------+


Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

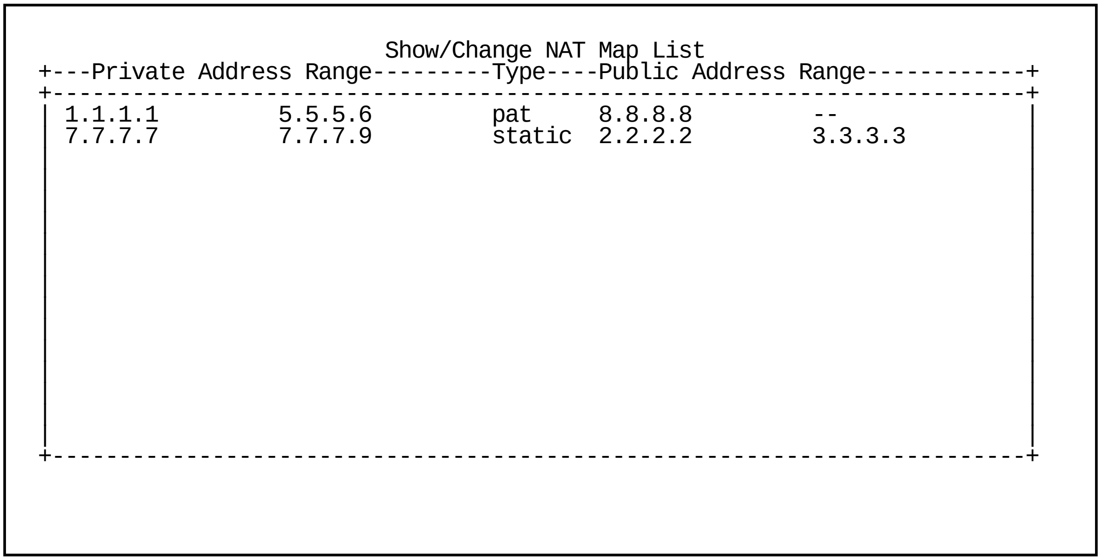
The Show/Change NAT Map List screen appears.



```
                          Show/Change NAT Map List

         Map List Name:                           my_map

         Add Map...

         Show/Change Maps...

         Delete Map...

         Move Map...
```

- **Add Map** allows you to add a new map to the map list.
- **Show/Change Maps** allows you to modify the individual maps within the list.
- **Delete Map** allows you to delete a map from the list.
- **Move Map** allows you to change the priority order in which the map is evaluated within the list. See “Moving maps” on page 10-12.

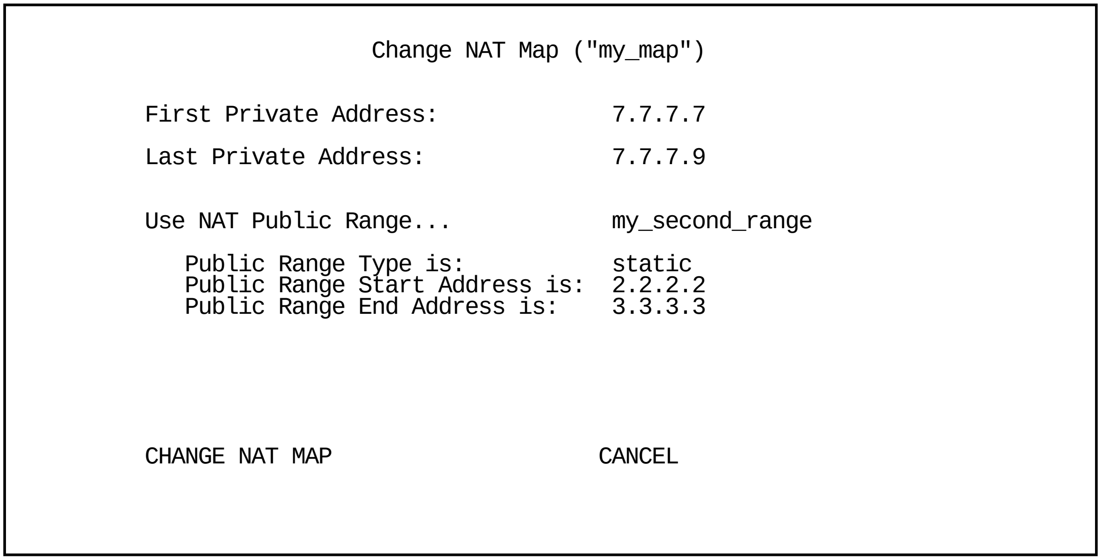
Selecting **Show/Change Maps**, **Delete Map**, or **Move Map** displays the same pop-up menu.



```
                          Show/Change NAT Map List
  +---Private Address Range---------Type----Public Address Range------------+
  +-------------------------------------------------------------------------+
  | 1.1.1.1         5.5.5.6         pat     8.8.8.8         --              |
  | 7.7.7.7         7.7.7.9         static  2.2.2.2         3.3.3.3         |
  |                                                                         |
  |                                                                         |
  |                                                                         |
  |                                                                         |
  |                                                                         |
  |                                                                         |
  |                                                                         |
  |                                                                         |
  |                                                                         |
  |                                                                         |
  |                                                                         |
  |                                                                         |
  +-------------------------------------------------------------------------+
```

Scroll to the map you want to modify using the arrow keys and press Return.

The Change NAT Map screen appears.

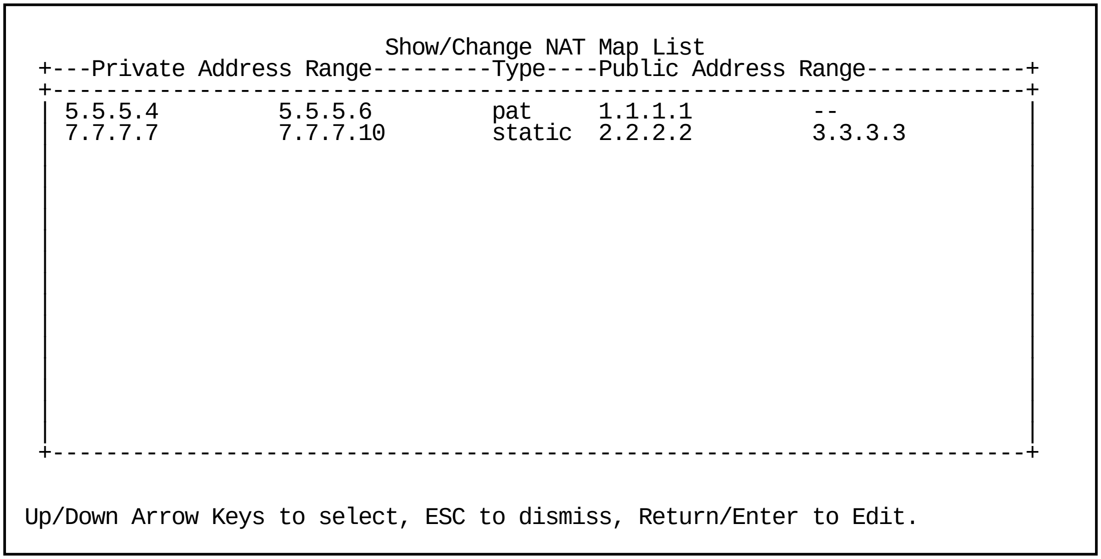


```
                            Change NAT Map ("my_map")

          First Private Address:             7.7.7.7

          Last Private Address:              7.7.7.9


          Use NAT Public Range...            my_second_range

             Public Range Type is:           static
             Public Range Start Address is:  2.2.2.2
             Public Range End Address is:    3.3.3.3




          CHANGE NAT MAP                    CANCEL
```

Make any modifications you need and then select **CHANGE NAT MAP** and press Return. Your changes will become effective and you will be returned to the Show/Change NAT Map List screen.

Moving maps

The Move Map screen permits reordering the priority of maps in a map list. If you used Easy Setup for your initial configuration, and added subsequent map and server lists, you may need to reorder their priority.



```
                             Show/Change NAT Map List
 +---Private Address Range---------Type----Public Address Range------------+
 +-------------------------------------------------------------------------+
 | 5.5.5.4         5.5.5.6         pat     1.1.1.1        --               |
 | 7.7.7.7         7.7.7.10        static  2.2.2.2        3.3.3.3          |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 +-------------------------------------------------------------------------+


Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

In the example screen above, you may want to reorder the priority of the maps such that the static map applies first and any additional traffic is routed via PAT.

All operations are done from a single pop-up menu.

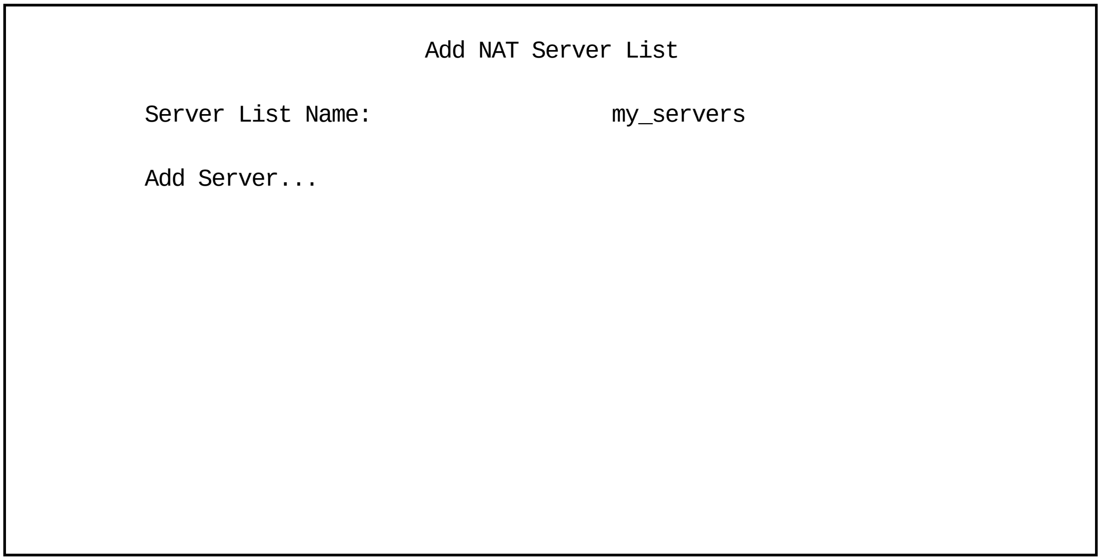
- In the Show/Change Map List screen, select **Move Map**. A selection mode pop-up menu appears. In this mode you scroll to the map you want to move and press Return to select it for moving.
- After pressing Return you are in Move mode. Arrow keys move the selected map up or down. When you press Return again the map is put in the new location permanently and the pop-up menu is dismissed. You can press Escape at any time in the pop-up menu to abort the move and restore the map list to its original ordering.

Adding server lists

Server lists, also known as Exports, are handled similarly to map lists. If you want to make a particular server's port accessible (and it isn't accessible through other means, such as a static mapping), you must create a Server List.

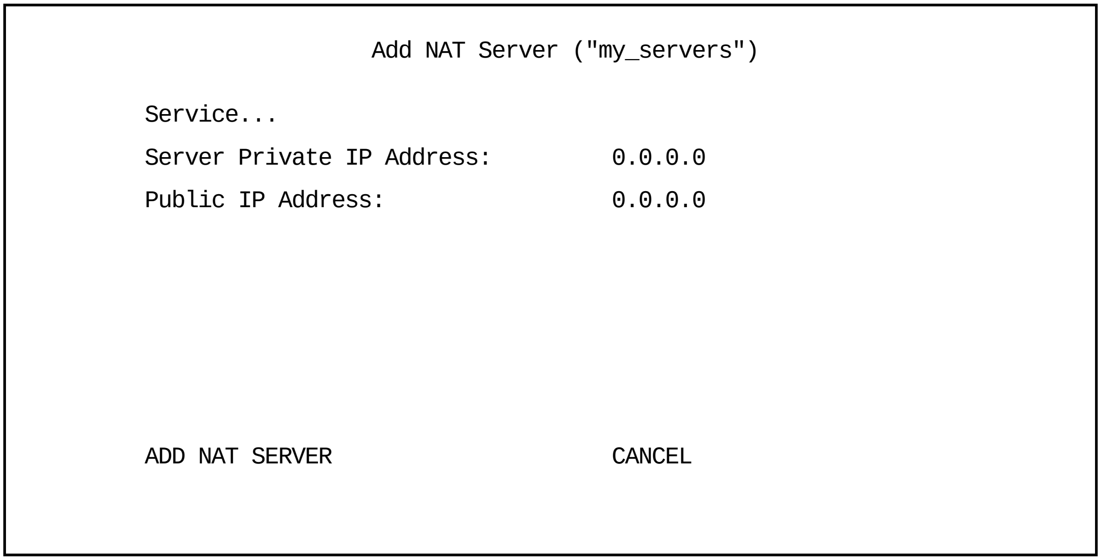
Select **Add Server List** from the Network Address Translation screen.

The Add NAT Server List screen appears.



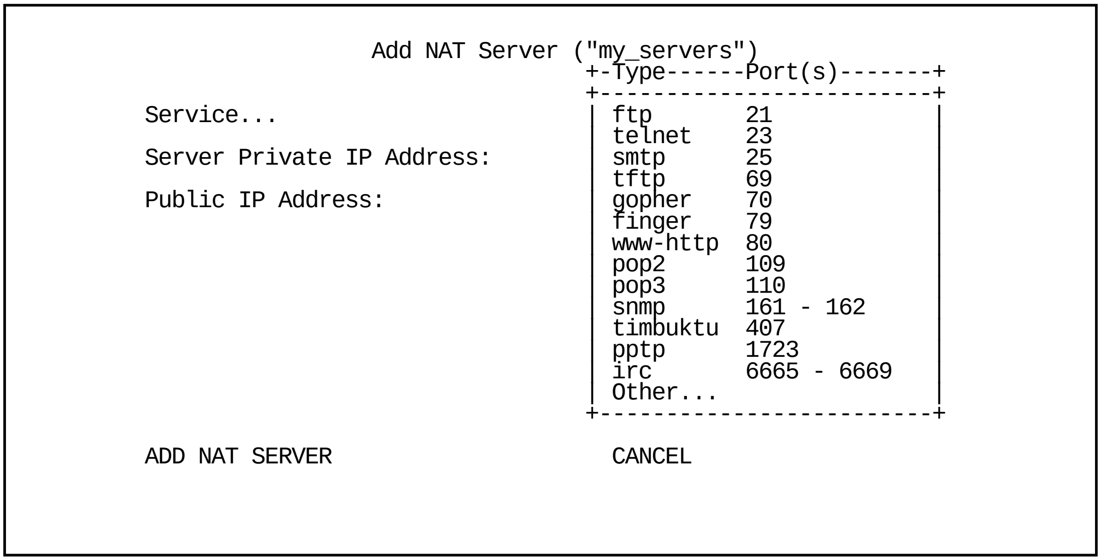
```
                        Add NAT Server List

      Server List Name:                 my_servers

      Add Server...
```

- Select **Server List Name** and type in a descriptive name. A new menu item, **Add Server**, appears.
- Select **Add Server** and press Return. The Add NAT Server screen appears.



```
                 Add NAT Server ("my_servers")

     Service...

     Server Private IP Address:          0.0.0.0

     Public IP Address:                  0.0.0.0









     ADD NAT SERVER                      CANCEL
```

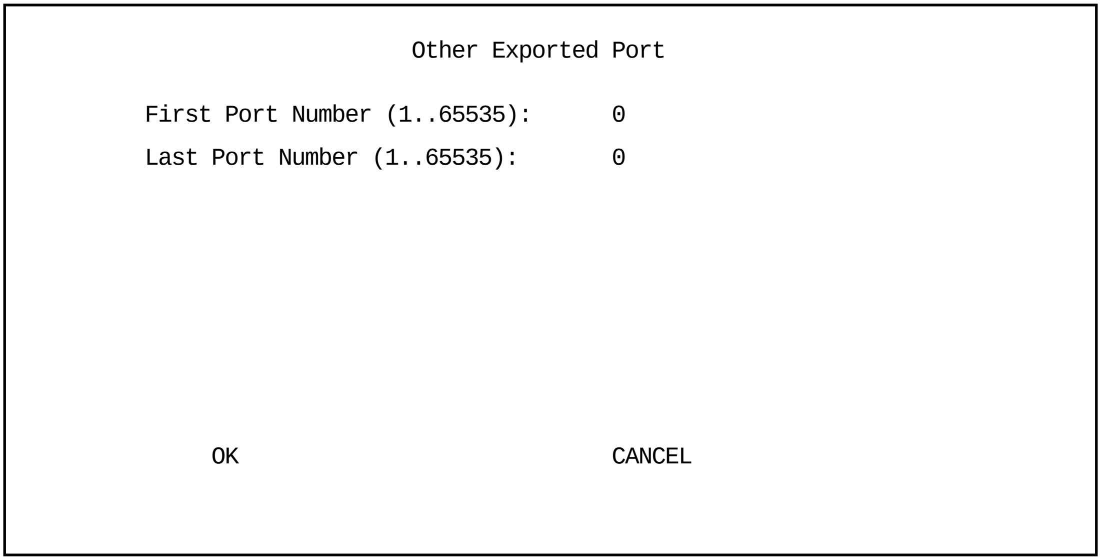
- Select **Service** and press Return. A pop-up menu appears listing a selection of commonly exported services.



```
                 Add NAT Server ("my_servers")
                                       +-Type------Port(s)-------+
                                       +-------------------------+
     Service...                        | ftp       21            |
                                       | telnet    23            |
     Server Private IP Address:        | smtp      25            |
                                       | tftp      69            |
     Public IP Address:                | gopher    70            |
                                       | finger    79            |
                                       | www-http  80            |
                                       | pop2      109           |
                                       | pop3      110           |
                                       | snmp      161 - 162     |
                                       | timbuktu  407           |
                                       | pptp      1723          |
                                       | irc       6665 - 6669   |
                                       | Other...                |
                                       +-------------------------+

     ADD NAT SERVER                      CANCEL
```

- Choose the service you want to export and press Return.

  You can choose a preconfigured service from the list, or define your own by selecting **Other**. If you select **Other**, a screen is displayed that allows you to enter the port number range for your customized service.



```
                         Other Exported Port

          First Port Number (1..65535):      0
          Last Port Number (1..65535):       0










               OK                            CANCEL
```

- Enter the **First** and **Last Port Number** between ports 1 and 65535. Select **OK** and press Return. You will be returned to the Add NAT Server screen.

- Enter the **Server Private IP Address** of the server whose service you are exporting.

  Since MultiNAT permits the mapping of multiple private IP addresses to multiple public IP addresses, your ISP or corporate site's router must be configured such that it knows that your multiple public addresses correspond to multiple private addresses on your router.

  If you want to use static mappings to map internal servers to public addresses, your ISP or corporate site's router must also be configured for static routes to these public addresses on the Netopia Router.

- Enter the **Public IP Address** to which you are exporting the service.

  Note: For PAT Map lists and Server lists, if you use the Public Address 0.0.0.0, the list will acquire its public IP address from the WAN IP address specified by your WAN IP configuration in the Connection Profile. If that is a static IP address, then the PAT map list and Server lists will acquire that address. If it is a negotiated IP address, such as may be assigned via DHCP or PPP, the PAT map list and Server lists will acquire that address each time it is negotiated.

- Select **ADD NAT SERVER** and press Return. The server will be added to your server list and you will be returned to the Add NAT Server List screen.

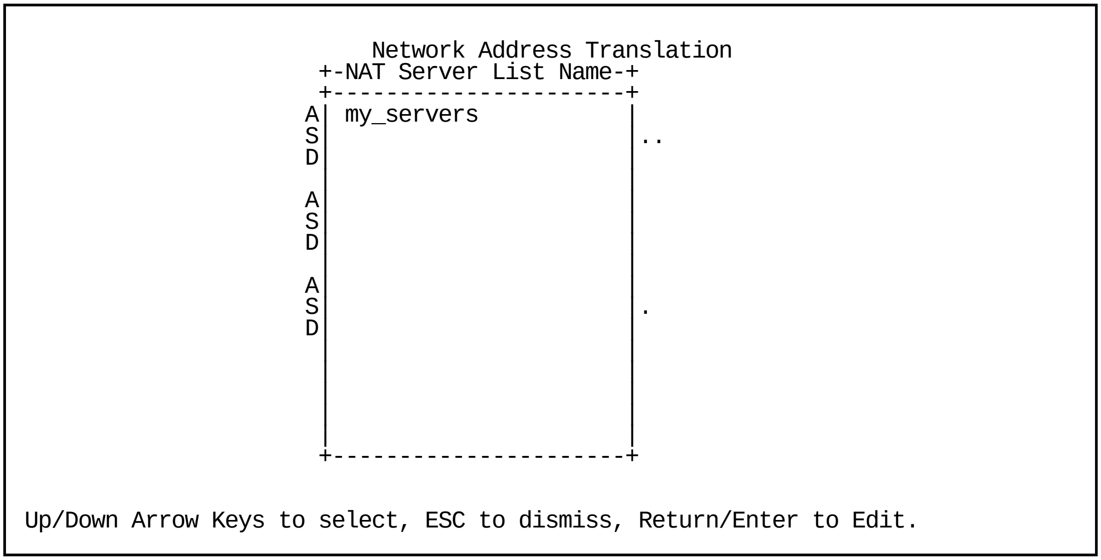
Note: CUSeeMe (or other services that listen on specific ports) through MultiNAT works as it did for regular NAT routers. In order to use CUSeeMe through the Netopia R2020 Router, you must export the ports 7648 *and* 7649. In MultiNAT, you may use a port range export. Without the export, CUSeeMe will fail to work.

Modifying server lists

Once a server list exists, you can select it for modification or deletion.

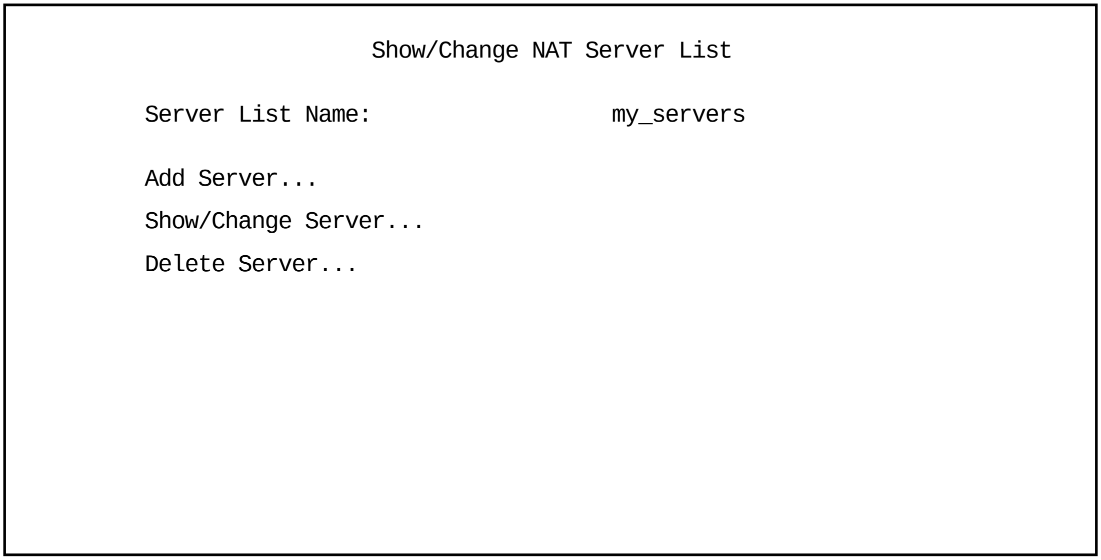
- Select **Show/Change Server List** from the Network Address Translation screen.

- Select the Server List Name you want to modify from the pop-up menu and press Return.



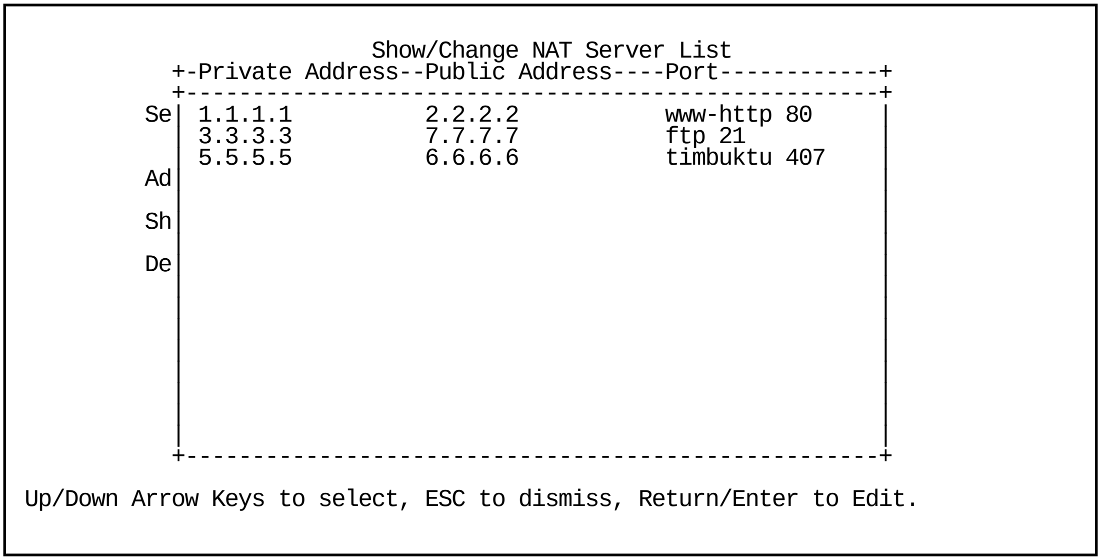
```
                              Network Address Translation
                          +-NAT Server List Name-+
                          +----------------------+
                         A| my_servers           |
                         S|                      |..
                         D|                      |
                          |                      |
                         A|                      |
                         S|                      |
                         D|                      |
                          |                      |
                         A|                      |
                         S|                      |.
                         D|                      |
                          |                      |
                          |                      |
                          |                      |
                          |                      |
                          +----------------------+


Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

The Show/Change NAT Server List screen appears.



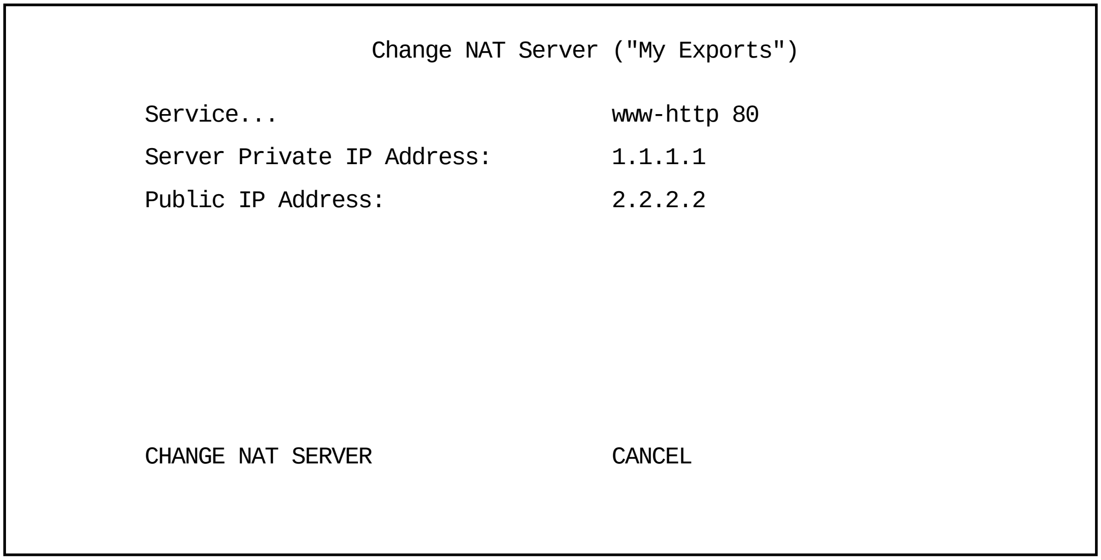
```
                              Show/Change NAT Server List

         Server List Name:                  my_servers

         Add Server...

         Show/Change Server...

         Delete Server...
```

- Selecting **Show/Change Server** or **Delete Server** displays the same pop-up menu.



```
                      Show/Change NAT Server List
           +-Private Address--Public Address----Port------------+
           +----------------------------------------------------+
         Se| 1.1.1.1          2.2.2.2            www-http 80     |
           | 3.3.3.3          7.7.7.7            ftp 21          |
           | 5.5.5.5          6.6.6.6            timbuktu 407    |
         Ad|                                                     |
           |                                                     |
         Sh|                                                     |
           |                                                     |
         De|                                                     |
           |                                                     |
           |                                                     |
           |                                                     |
           |                                                     |
           |                                                     |
           |                                                     |
           |                                                     |
           +----------------------------------------------------+

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

Select any server from the list and press Return. The Change NAT Server screen appears.



```
                      Change NAT Server ("My Exports")

         Service...                        www-http 80

         Server Private IP Address:        1.1.1.1

         Public IP Address:                2.2.2.2










         CHANGE NAT SERVER                 CANCEL
```

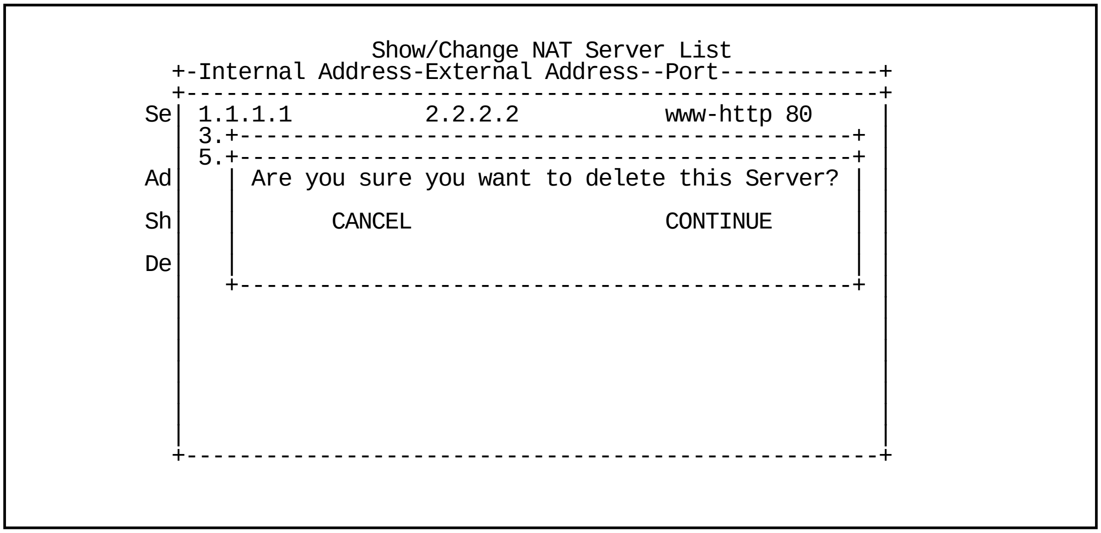
You can make changes to the server's service and port or internal or external address.

Select **CHANGE NAT SERVER** and press Return. Your changes take effect and you are returned to the Show/Change NAT Server List screen.

Deleting a server

To delete a server from the list, select **Delete Server** from the Show/Change NAT Server List menu and press Return.

A pop-up menu lists your configured servers. Select the one you want to delete and press Return. A dialog box asks you to confirm your choice.



```
                        Show/Change NAT Server List
     +-Internal Address-External Address--Port------------+
     +----------------------------------------------------+
   Se| 1.1.1.1          2.2.2.2          www-http 80      |
     | 3.+----------------------------------------------+ |
     | 5.+----------------------------------------------+ |
   Ad|   | Are you sure you want to delete this Server? | |
     |   |                                              | |
   Sh|   |       CANCEL                   CONTINUE      | |
     |   |                                              | |
   De|   |                                              | |
     |   +----------------------------------------------+ |
     |                                                    |
     |                                                    |
     |                                                    |
     |                                                    |
     |                                                    |
     |                                                    |
     +----------------------------------------------------+
```

Choose **CONTINUE** and press Return. The server is deleted from the list.

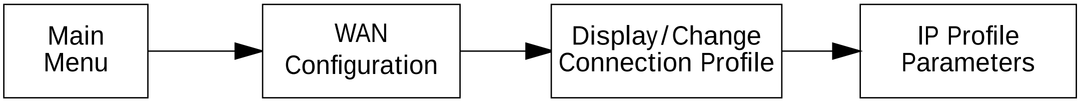
Binding Map Lists and Server Lists

Once you have created your map lists and server lists, you must bind them to a profile, either a Connection Profile or the Default Profile. You do this in one of the following screens:

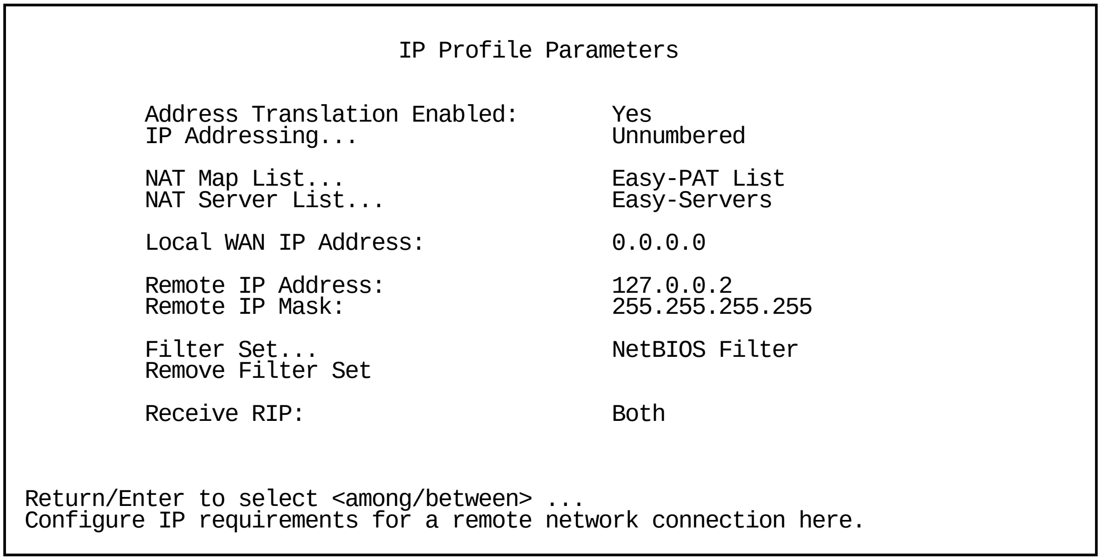
- the IP profile parameters screen (see below) of the Connection Profile configuration menu
- the Default Answer Profile screen (see page 10-20)

IP profile parameters

To bind a map list to a Connection Profile, from the Main Menu go to the WAN Configuration screen then the Display/Change Connection Profile screen. From the pop-up menu list of your Connection Profiles, choose the one you want to bind your map list to. Select **IP Profile Parameters** and press Return.

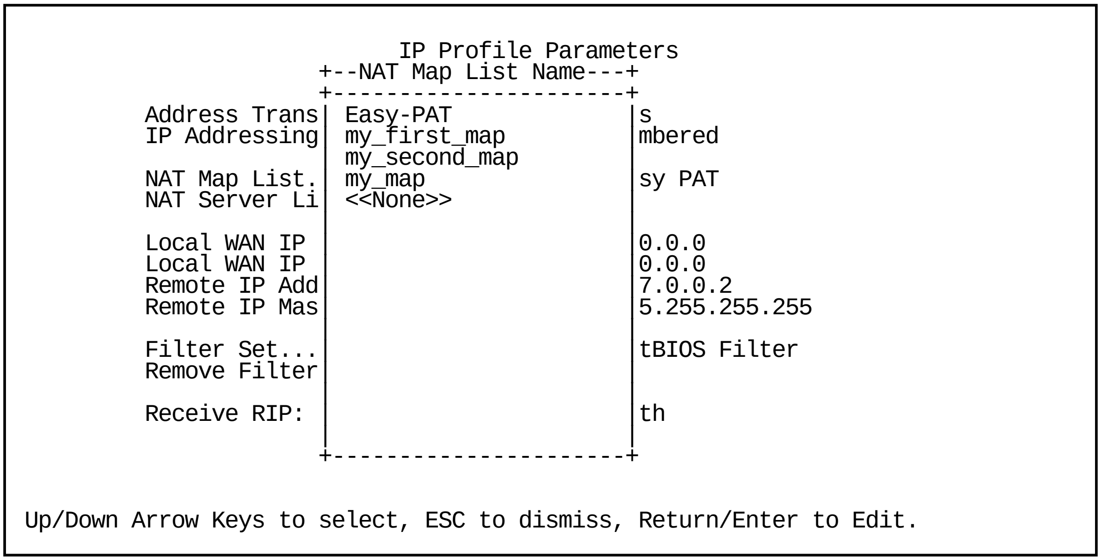


The IP Profile Parameters screen appears.



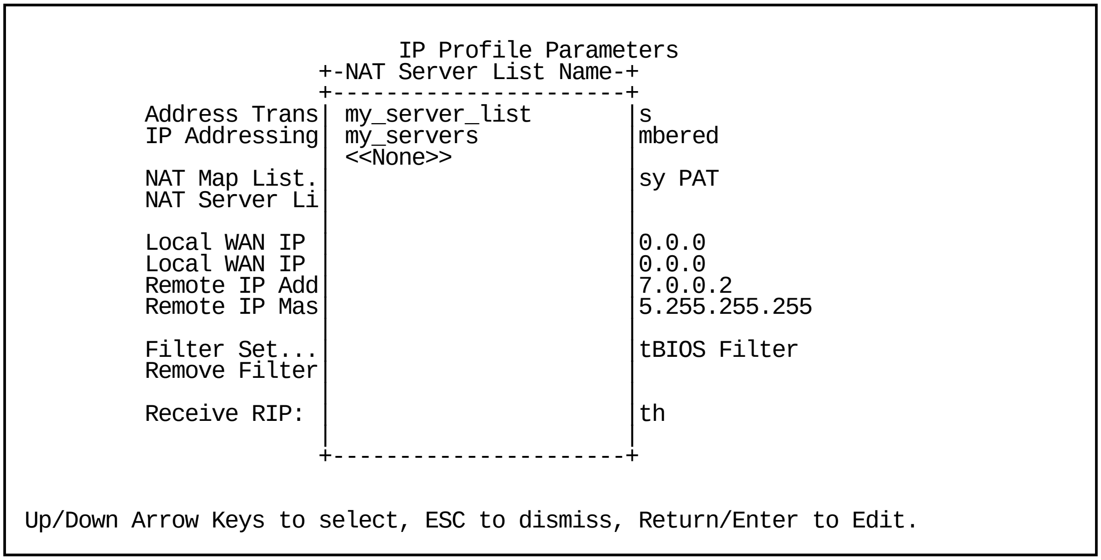
```
                            IP Profile Parameters

         Address Translation Enabled:       Yes
         IP Addressing...                   Unnumbered

         NAT Map List...                    Easy-PAT List
         NAT Server List...                 Easy-Servers

         Local WAN IP Address:              0.0.0.0

         Remote IP Address:                 127.0.0.2
         Remote IP Mask:                    255.255.255.255

         Filter Set...                      NetBIOS Filter
         Remove Filter Set

         Receive RIP:                       Both



Return/Enter to select <among/between> ...
Configure IP requirements for a remote network connection here.
```

- Select **NAT Map List** and press Return. A pop-up menu displays a list of your defined map lists.



```
                            IP Profile Parameters
                      +--NAT Map List Name---+
                      +----------------------+
         Address Trans| Easy-PAT             |s
         IP Addressing| my_first_map         |mbered
                      | my_second_map        |
         NAT Map List.| my_map               |sy PAT
         NAT Server Li| <<None>>             |
                      |                      |
         Local WAN IP |                      |0.0.0
         Local WAN IP |                      |0.0.0
         Remote IP Add|                      |7.0.0.2
         Remote IP Mas|                      |5.255.255.255
                      |                      |
         Filter Set...|                      |tBIOS Filter
         Remove Filter|                      |
                      |                      |
         Receive RIP: |                      |th
                      |                      |
                      +----------------------+


Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

- Select the map list you want to bind to this Connection Profile and press Return. The map list you selected will now be bound to this Connection Profile.
- Select **NAT Server List** and press Return. A pop-up menu displays a list of your defined server lists.



```
                          IP Profile Parameters
                    +-NAT Server List Name-+
                    +----------------------+
         Address Trans| my_server_list       |s
         IP Addressing| my_servers           |mbered
                      | <<None>>             |
         NAT Map List.|                      |sy PAT
         NAT Server Li|                      |
                      |                      |
         Local WAN IP |                      |0.0.0
         Local WAN IP |                      |0.0.0
         Remote IP Add|                      |7.0.0.2
         Remote IP Mas|                      |5.255.255.255
                      |                      |
         Filter Set...|                      |tBIOS Filter
         Remove Filter|                      |
                      |                      |
         Receive RIP: |                      |th
                      |                      |
                    +----------------------+


Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

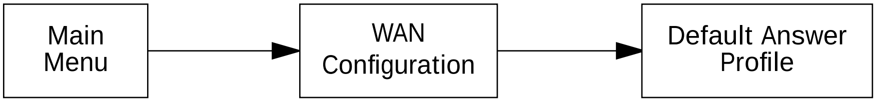
- Select the server list you want to bind to this Connection Profile and press Return. The server list you selected will now be bound to this Connection Profile.

Note: There is no interdependency between NAT and IP Addressing. Also, the Local WAN IP Address and Mask fields' visibility are dependent only on the IP Addressing type.

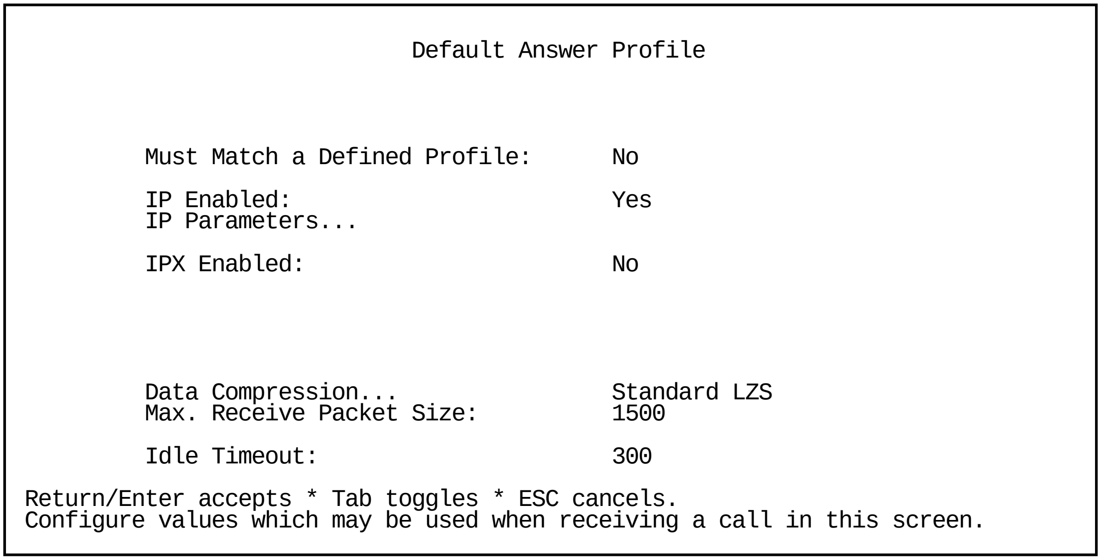
Default Answer Profile

When using the default answer profile for dial-in connections, the procedure is similar to binding map lists and server lists to a Connection Profile.

From the Main Menu go to the WAN Configuration screen, then the WAN (Wide Area Network) Setup screen. Select **Default Answer Profile** and press Return.



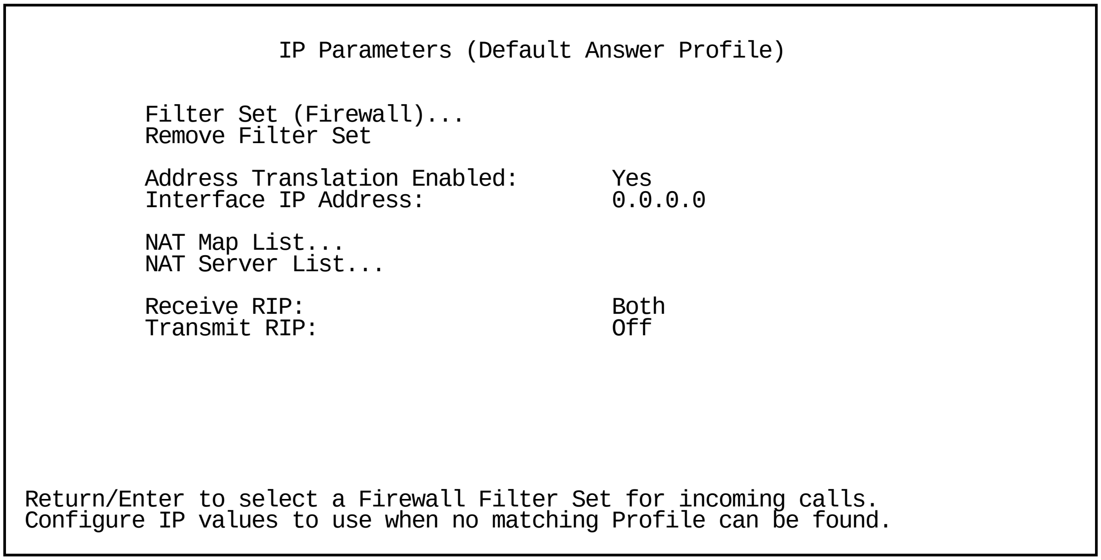
The Default Answer Profile screen appears.



```
                             Default Answer Profile



         Must Match a Defined Profile:      No

         IP Enabled:                        Yes
         IP Parameters...

         IPX Enabled:                       No





         Data Compression...                Standard LZS
         Max. Receive Packet Size:          1500

         Idle Timeout:                      300

Return/Enter accepts * Tab toggles * ESC cancels.
Configure values which may be used when receiving a call in this screen.
```

If **Must Match a Defined Profile** is set to **Yes**, then the NAT attributes of the Connection Profile take precedence. If you toggle **Must Match a Defined Profile** to **No**, IP-related menu options become visible.

- Select **IP Parameters** and press Return. The IP Parameters (Default Answer Profile) screen appears.



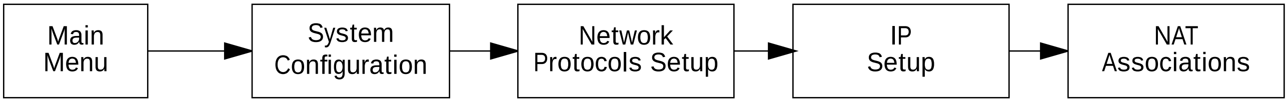
```
                   IP Parameters (Default Answer Profile)


         Filter Set (Firewall)...
         Remove Filter Set

         Address Translation Enabled:       Yes
         Interface IP Address:              0.0.0.0

         NAT Map List...
         NAT Server List...

         Receive RIP:                       Both
         Transmit RIP:                      Off






Return/Enter to select a Firewall Filter Set for incoming calls.
Configure IP values to use when no matching Profile can be found.
```

You can then bind NAT Map Lists and NAT Server Lists in the same fashion as described in the section "IP profile parameters" on page 10-18.

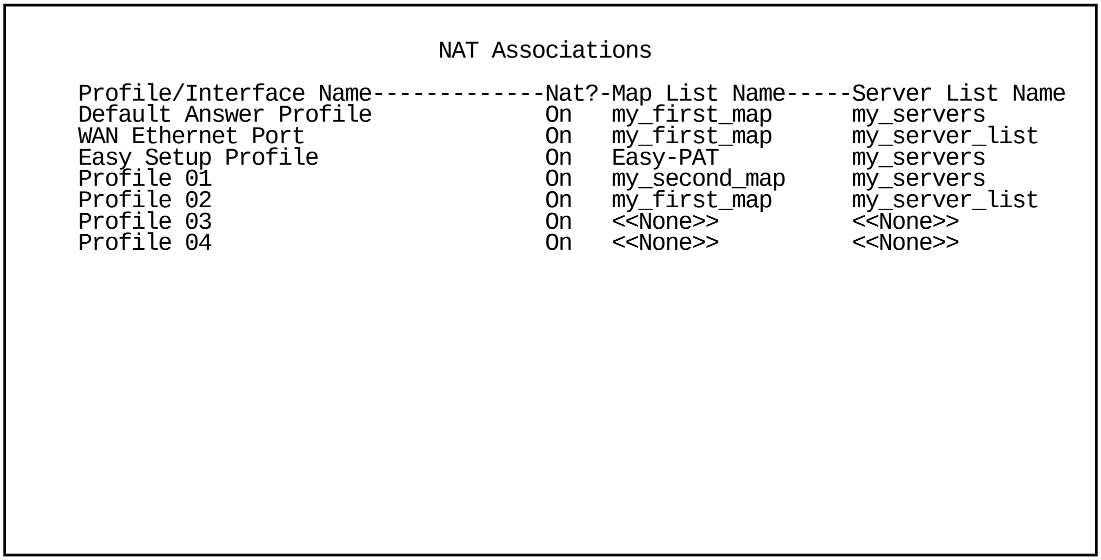
NAT Associations

Configuration of map and server lists alone is not sufficient to enable NAT for a WAN connection because map and server lists must be linked to a profile that controls the WAN interface. This can be a Connection Profile, a WAN Ethernet interface, a default profile, or a default answer profile. Once you have configured your map and server lists, you may want to reassign them to different interface-controlling profiles, for example, Connection Profiles. To permit easy access to this IP Setup functionality, you can use the NAT Associations screen.

You access the NAT Associations screen from the Network Address Translation screen.

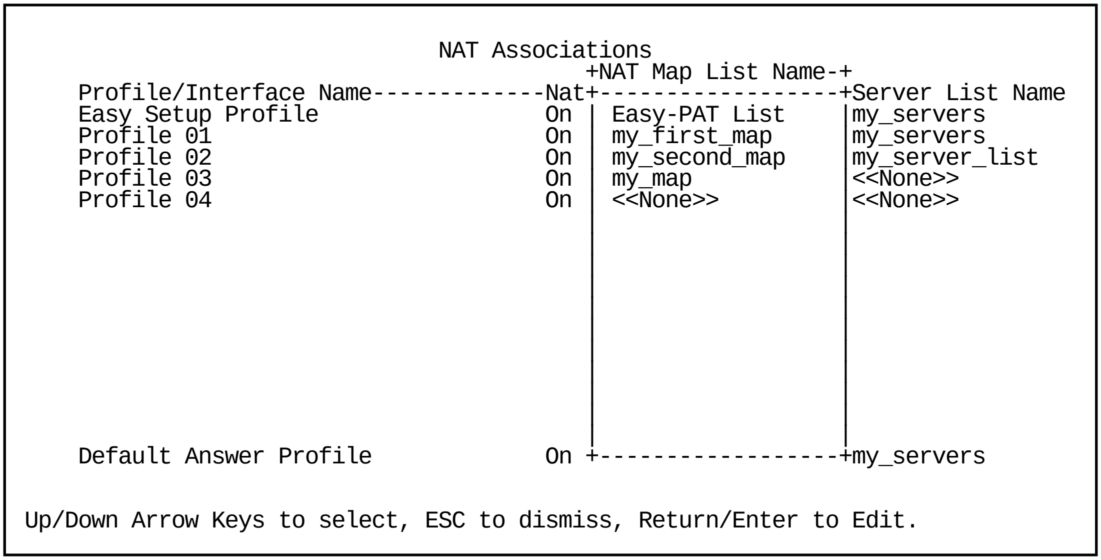


Select **NAT Associations** and press Return. The NAT Associations screen appears.



```
                               NAT Associations

    Profile/Interface Name-------------Nat?-Map List Name-----Server List Name
    Default Answer Profile             On   my_first_map      my_servers
    WAN Ethernet Port                  On   my_first_map      my_server_list
    Easy Setup Profile                 On   Easy-PAT          my_servers
    Profile 01                         On   my_second_map     my_servers
    Profile 02                         On   my_first_map      my_server_list
    Profile 03                         On   <<None>>          <<None>>
    Profile 04                         On   <<None>>          <<None>>
```

- You can toggle **NAT? On** or **Off** for each Profile/Interface name. You do this by navigating to the **NAT?** field associated with each profile using the arrow keys. Toggle NAT on or off by using the Tab key.
- You can reassign any of your map lists or server lists to any of the Profile/Interfaces. You do this by navigating to the **Map List Name** or **Server List Name** field associated with each profile using the arrow keys. Select the item by pressing Return to display a pop-up menu of all of your configured lists.



```
                               NAT Associations
                                          +NAT Map List Name-+
    Profile/Interface Name-------------Nat+------------------+Server List Name
    Easy Setup Profile                 On | Easy-PAT List    |my_servers
    Profile 01                         On | my_first_map     |my_servers
    Profile 02                         On | my_second_map    |my_server_list
    Profile 03                         On | my_map           |<<None>>
    Profile 04                         On | <<None>>         |<<None>>
                                          |                  |
                                          |                  |
                                          |                  |
                                          |                  |
                                          |                  |
                                          |                  |
                                          |                  |
                                          |                  |
                                          |                  |
                                          |                  |
    Default Answer Profile             On +------------------+my_servers

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

- Select the list name you want to assign and press Return again. Your selection will then be associated with the corresponding profile or interface.

MultiNAT Configuration Example

To help you understand a typical MultiNAT configuration, this section describes an example of the type of configuration you may want to implement on your site. The values shown are for example purposes only. *Make your own appropriate substitutions.*

A typical service from an ISP might include five user addresses. Without PAT, you might be able to attach only five IP hosts. Using simple 1-to-many PAT you can connect more than five devices, but use only one of your addresses. Using multiNAT you can make full use of the address range. The example assumes the following range of addresses offered by a typical ISP:

Local WAN IP address:	173.166.100.34
Local WAN subnet mask:	255.255.255.252
Remote IP address:	173.166.100.33
Default gateway:	173.166.100.33

Public IP addresses assigned by the ISP are 206.1.1.1 through 206.1.1.6 (255.255.255.248 subnet mask).

Your internal devices have IP addresses of 192.168.1.1 through 192.168.1.254 (255.255.255.0 subnet mask).

Netopia router's address is:	192.168.1.1
Web server's address is:	192.168.1.2
Mail server's address is:	192.168.1.3
FTP server's address is:	192.168.1.4

In this example you will statically map the first five public IP addresses (206.1.1.1 - 206.1.1.5) to the first five corresponding private IP addresses (192.168.1.1 - 192.168.1.5). You will use these 1-to-1 mapped addresses to give your servers “real” addresses. You will then map 206.1.1.6 to the remaining private IP addresses (192.168.1.6 - 192.168.1.254) using PAT.

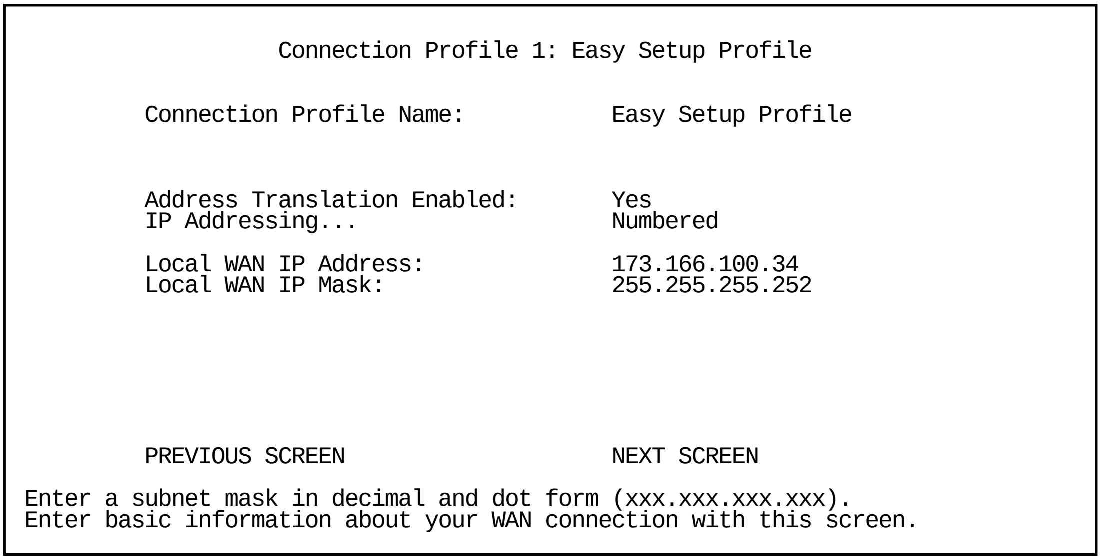
Note: The public side needs a static route indicating that to get to 206.1.1.1 - 206.1.1.5, it is necessary to go through 173.166.100.34.

The configuration process is as follows:

From the Main Menu go to the Easy Setup and then the Connection Profile screen.

Main Menu
Easy Setup
Connection Profile

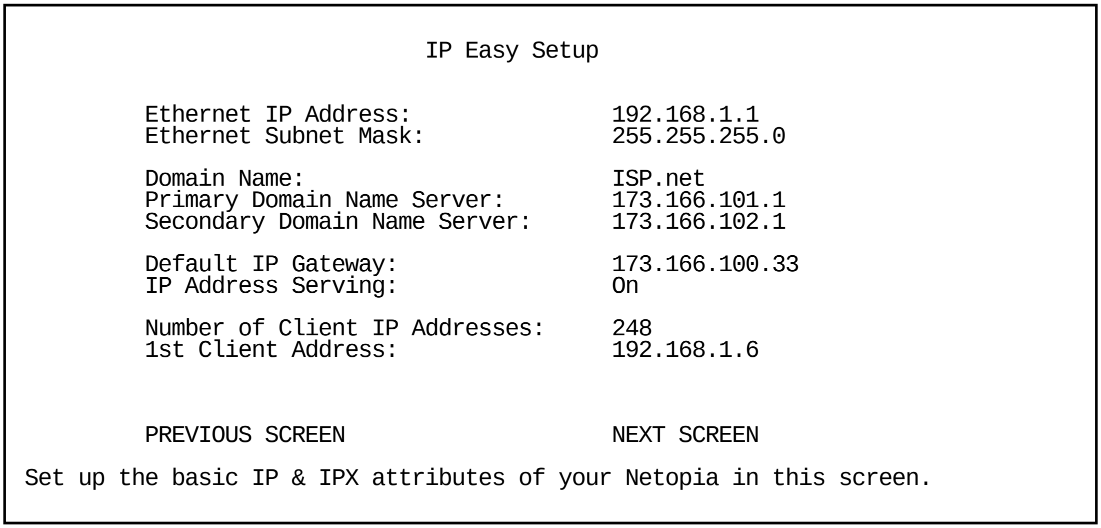
Enter your ISP-supplied values as shown below.



```
                     Connection Profile 1: Easy Setup Profile

         Connection Profile Name:            Easy Setup Profile



         Address Translation Enabled:        Yes
         IP Addressing...                    Numbered

         Local WAN IP Address:               173.166.100.34
         Local WAN IP Mask:                  255.255.255.252







         PREVIOUS SCREEN                     NEXT SCREEN

Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).
Enter basic information about your WAN connection with this screen.
```

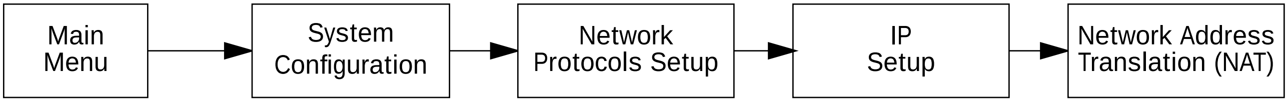
Select **NEXT SCREEN** and press Return.

Your IP values are shown here.

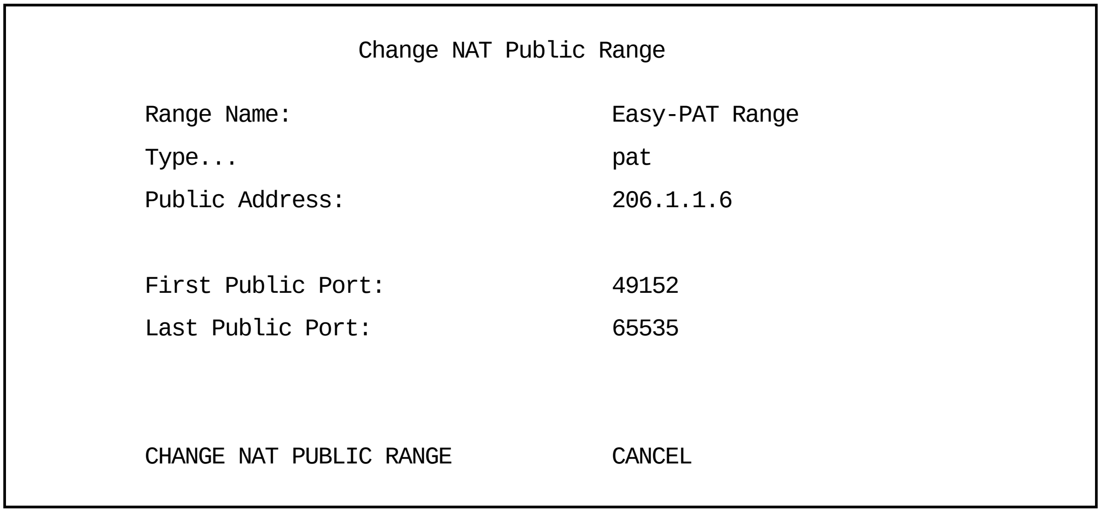


```
                                IP Easy Setup

         Ethernet IP Address:                192.168.1.1
         Ethernet Subnet Mask:               255.255.255.0

         Domain Name:                        ISP.net
         Primary Domain Name Server:         173.166.101.1
         Secondary Domain Name Server:       173.166.102.1

         Default IP Gateway:                 173.166.100.33
         IP Address Serving:                 On

         Number of Client IP Addresses:      248
         1st Client Address:                 192.168.1.6



         PREVIOUS SCREEN                     NEXT SCREEN

Set up the basic IP & IPX attributes of your Netopia in this screen.
```

Then navigate to the Network Address Translation (NAT) screen.



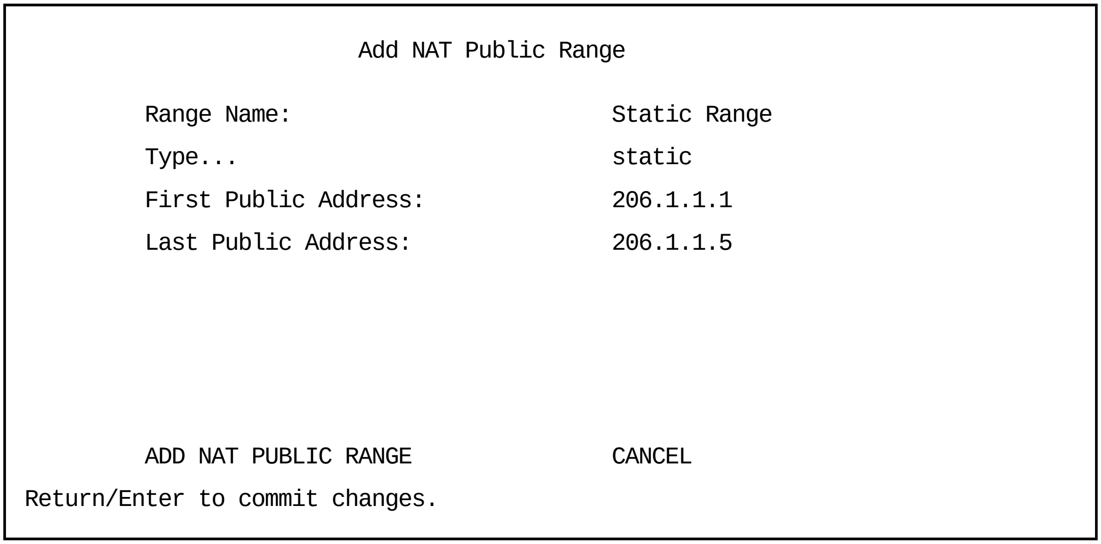
Select **Show / Change Public Range**, then **Easy-PAT Range**, and press Return. Enter the value your ISP assigned for your public address (206.1.1.6, in this example). Toggle **Type** to *pat*. Your public address is then mapped to the remaining private IP addresses using PAT. (If you were not using the Easy-PAT Range and Easy-PAT List that is created by default by using Easy Setup, you would have to *define* a public range and Map List. For the purpose of this example you can just *alter* this range and list.)



```
                           Change NAT Public Range

          Range Name:                        Easy-PAT Range

          Type...                            pat

          Public Address:                    206.1.1.6


          First Public Port:                 49152

          Last Public Port:                  65535




          CHANGE NAT PUBLIC RANGE            CANCEL
```

Select **CHANGE NAT PUBLIC RANGE** and press Return. This returns you to the Network Address Translation screen.

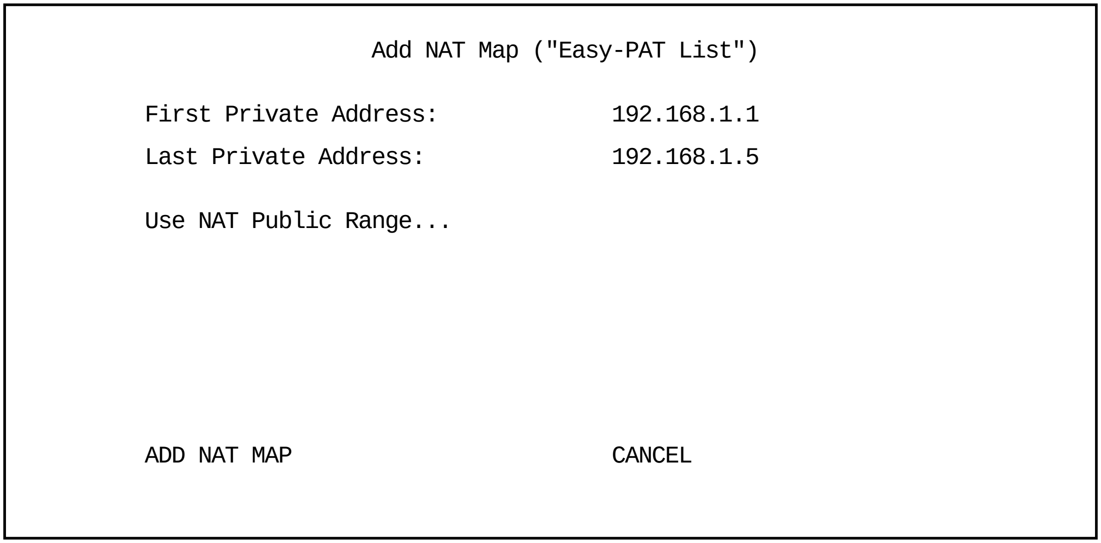
Select **Add Public Range** and press Return. Type a name for this static range, as shown below. Enter the first and last public addresses your ISP assigned in their respective fields as shown. The first five public IP addresses (206.1.1.1 - 206.1.1.5, in this example) are statically mapped to the first five corresponding private IP addresses (192.168.1.1 - 192.168.1.5).



```
                           Add NAT Public Range

          Range Name:                        Static Range

          Type...                            static

          First Public Address:              206.1.1.1

          Last Public Address:               206.1.1.5






          ADD NAT PUBLIC RANGE               CANCEL

 Return/Enter to commit changes.
```

Select **ADD NAT PUBLIC RANGE** and press Return. You are returned to the **Network Address Translation** screen.

Next, select **Show/Change Map List** and choose **Easy-PAT List**. Select **Add Map**. The **Add NAT Map** screen appears. (Now the name *Easy-PAT List* is a misnomer since it has a static map included in its list.) Enter in 192.168.1.1 for the **First Private Address** and 192.168.1.5 for the **Last Private Address**.



```
                        Add NAT Map ("Easy-PAT List")

          First Private Address:             192.168.1.1
          Last Private Address:              192.168.1.5

          Use NAT Public Range...






          ADD NAT MAP                        CANCEL
```

Select **Use NAT Public Range** and from the pop-up menu choose **Static Range**. Select **ADD NAT MAP** and press Return.

This will statically map the first five public IP addresses to the first five corresponding private IP addresses and will map 206.1.1.6 to the remaining private IP addresses using PAT.

Notes on the example

The Easy-Map List and the Easy-PAT List are attached to any new Connection Profile by default. If you want to use this NAT configuration on a previously defined Connection Profile then you need to *bind* the Map List to the profile. You do this through either the NAT Associations screen or the profile's configuration screens.

The PAT part of this example setup will allow any user on the Netopia Router's LAN with an IP address in the range of 192.168.1.6 through 192.168.1.254 to *initiate* traffic flow to the outside world (for example, the Internet). No one on the Internet would be able to initiate a conversation with them.

The Static Remapping part of this example will allow any of the machines in the range of addresses from 192.168.1.1 through 192.168.1.5 to communicate with the outside world as if they were at the addresses 206.1.1.1 through 206.1.1.5, respectively. It also allows any machine on the Internet to access any service (port) on any of these five machines.

You may decide this poses a security risk. You may decide that anyone can have complete access to your FTP server, but not to your router, and only limited access to the desired services (ports) on the Web and Mail servers.

To make these changes, first limit the range of remapped addresses on the Static Map and then edit the default Server List called Easy-Servers.

- First, navigate to the **Show/Change Map List** screen, select **Easy-PAT List** and then **Show/Change Maps**. Choose the **Static Map** you created and change the **First Private Address** from 192.168.1.1 to 192.168.1.4. Now the router, Web, and Mail servers' IP addresses are no longer included in the range of static remappings and are therefore no longer accessible to the outside world. Users on the Internet will not be able to telnet, web, SNMP or ping to them. It is best also to navigate to the public range screen and change the **Static Range** to go from 206.1.1.5.
- Next, navigate to **Show/Change Server List** and select **Easy-Servers** and then **Add Server**. You should export both the Web (www-http) and Mail (smtp) ports to one of the now free public addresses. Select **Service...** and from the resulting pop-up menu select **www-http**. In the resulting screen enter your Web server's address, 192.168.1.2 and the public address, for example, 206.1.1.2 and then select **ADD NAT SERVER**. Now return to **Add Server**, choose the **smtp** port and enter 192.168.1.3, your Mail server's IP address for the **Server Private IP Address**. You can decide if you want to present both your Web and Mail services as being on the same public address, 206.1.1.2, or if you prefer to have your Mail server appear to be at a different IP address, 206.1.1.3. For the sake of this example, alias both services to 206.1.1.2.

Now, as before, the PAT configuration will allow any user on the Netopia Router's LAN with an IP address in the range of 192.168.1.6 through 192.168.1.254 to initiate traffic flow to the Internet. Someone at the FTP server can access the Internet and the Internet can access all services of the FTP machine as if it were at 206.1.1.5. The router cannot directly communicate with the outside world. The only communication between the Web server and the Internet is through port 80, the web port, as if the server were located on a machine at IP address 206.1.1.2. Similarly, the only communication with the Mail server is through port 25, the SMTP port, as if it were located at IP address 206.1.1.2

Firmware upgrades and NAT

If you are upgrading from an earlier firmware version, your previous NAT configuration will continue to work as you have configured it.

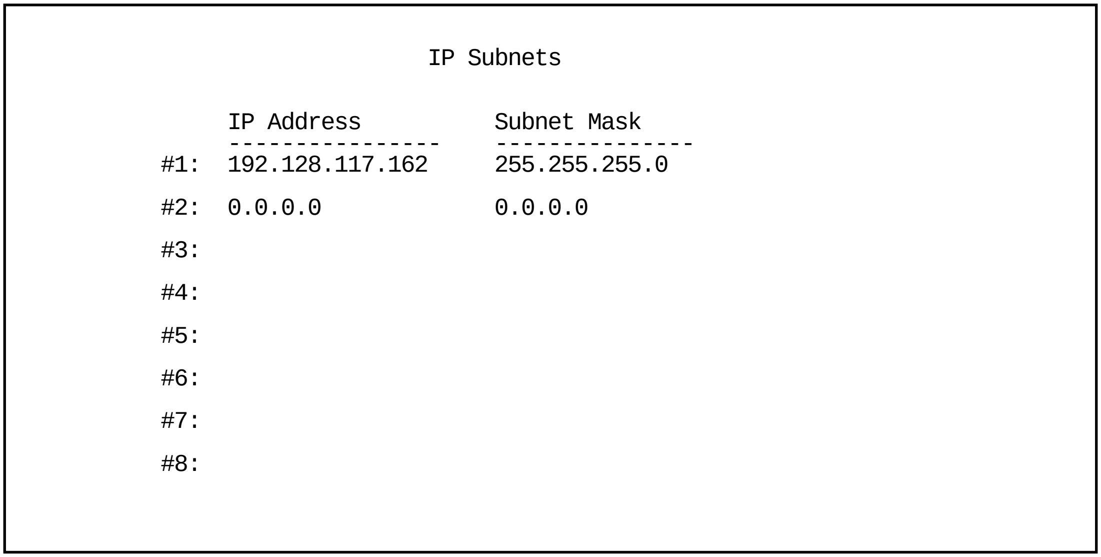
A NAT map list, and possibly a server list, will be created for each enabled profile that has NAT enabled. For each profile with a unique local WAN IP address, a single outside PAT public range will be created whose address is the profile's local WAN IP address. A map list will be created with as many maps as there are enabled subnets on the ethernet. Each of these maps will bind each subnet to the outside public range.

Likewise, if exports exist, a server list will be created for each NAT-enabled Connection Profile with a unique local WAN IP address that maps the interior server address and port to the local WAN IP address of the profile.

Both the map list and server list that applies to the particular profile will be bound to that profile.

IP subnets

The IP Subnets screen allows you to configure up to eight Ethernet IP subnets, one “primary” subnet and up to seven secondary subnets, by entering IP address/subnet mask pairs:



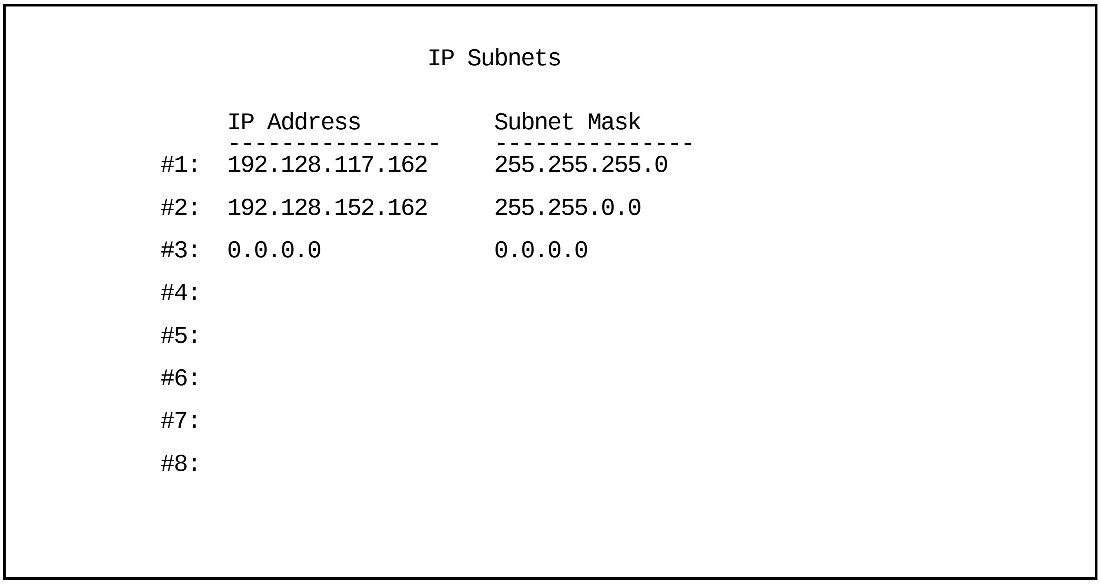
```
                        IP Subnets

              IP Address          Subnet Mask
              ----------------    ---------------
         #1:  192.128.117.162     255.255.255.0

         #2:  0.0.0.0             0.0.0.0

         #3:

         #4:

         #5:

         #6:

         #7:

         #8:
```

Note: You need not use this screen if you have only a single Ethernet IP subnet. In that case, you can continue to enter or edit the IP address and subnet mask for the single subnet on the IP Setup screen.

This screen displays up to eight rows of two editable columns, preceded by a row number between one and eight. If you have eight subnets configured, there will be eight rows on this screen. Otherwise, there will be one more row than the number of configured subnets. The last row will have the value 0.0.0.0 in both the IP address and subnet mask fields to indicate that you can edit the values in this row to configure an additional subnet. All eight row labels are always visible, regardless of the number of subnets configured.

- To add an IP subnet, enter the Netopia R2020’s IP address on the subnet in the **IP Address** field in a particular row and the subnet mask for the subnet in the **Subnet Mask** field in that row.

For example:

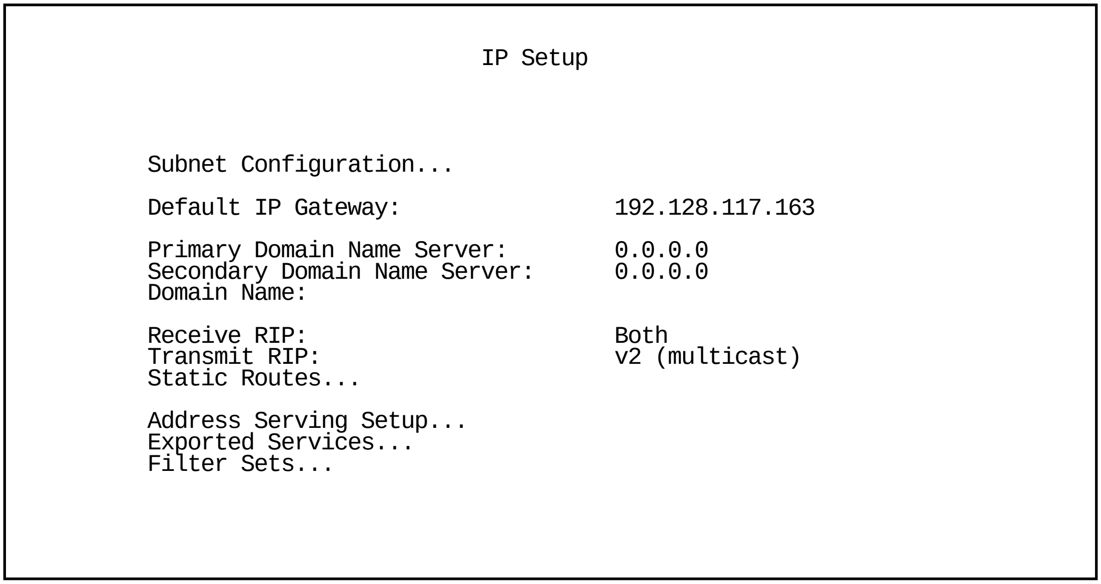


```
                              IP Subnets

           IP Address           Subnet Mask
           ----------------     ---------------
      #1:  192.128.117.162      255.255.255.0

      #2:  192.128.152.162      255.255.0.0

      #3:  0.0.0.0              0.0.0.0

      #4:

      #5:

      #6:

      #7:

      #8:
```

- To delete a configured subnet, set both the IP address and subnet mask values to 0.0.0.0, either explicitly or by clearing each field and pressing Return or Enter to commit the change. When a configured subnet is deleted, the values in subsequent rows adjust up to fill the vacant fields.

Note that the subnets configured on this screen are tied to the address serving pools configured on the IP Address Pools screen, and that changes on this screen may affect the IP Address Pools screen. In particular, deleting a subnet configured on this screen will delete the corresponding address serving pool, if any, on the IP Address Pools screen.

If you have configured multiple Ethernet IP subnets, the IP Setup screen changes slightly:



```
                                   IP Setup



          Subnet Configuration...

          Default IP Gateway:                  192.128.117.163

          Primary Domain Name Server:          0.0.0.0
          Secondary Domain Name Server:        0.0.0.0
          Domain Name:

          Receive RIP:                         Both
          Transmit RIP:                        v2 (multicast)
          Static Routes...

          Address Serving Setup...
          Exported Services...
          Filter Sets...
```

The IP address and Subnet mask items are hidden, and the “Define Additional Subnets...” item becomes “Subnet Configuration...”. If you select **Subnet Configuration**, you will return to the IP Subnets screen that allows you to define IP addresses and masks for additional Ethernet IP subnets.

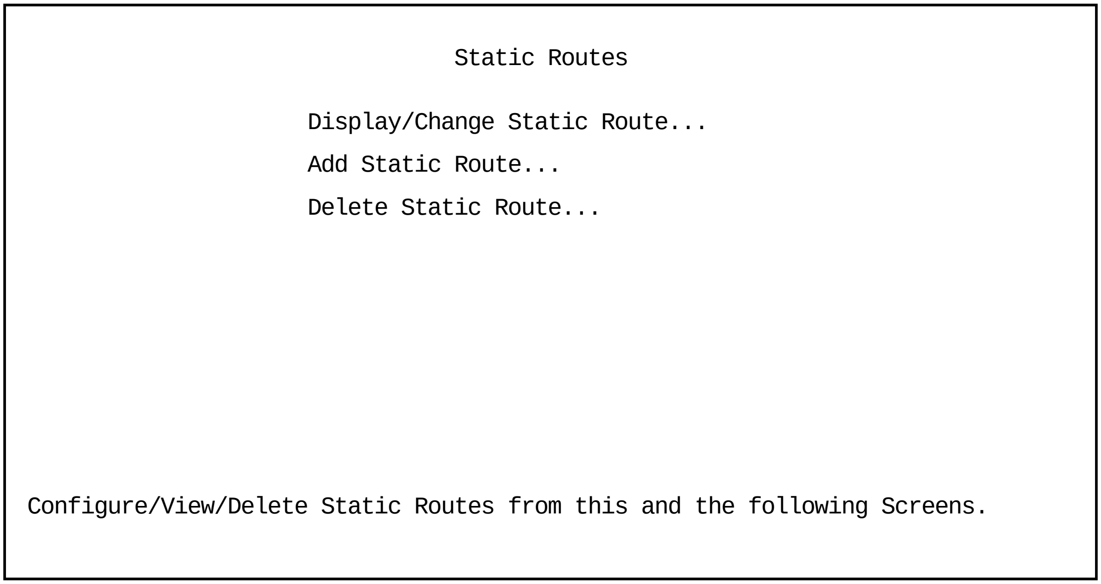
■ Select **Static Routes** to manually configure IP routes. See the following section.

Static routes

Static routes are IP routes that are maintained manually. Each static route acts as a pointer that tells the Netopia R2020 how to reach a particular network. However, static routes are used only if they appear in the IP routing table, which contains all of the routes used by the Netopia R2020 (see “IP routing table” on page 13-8).

Static routes are helpful in situations where a route to a network must be used and other means of finding the route are unavailable. For example, static routes are useful when you cannot rely on RIP.

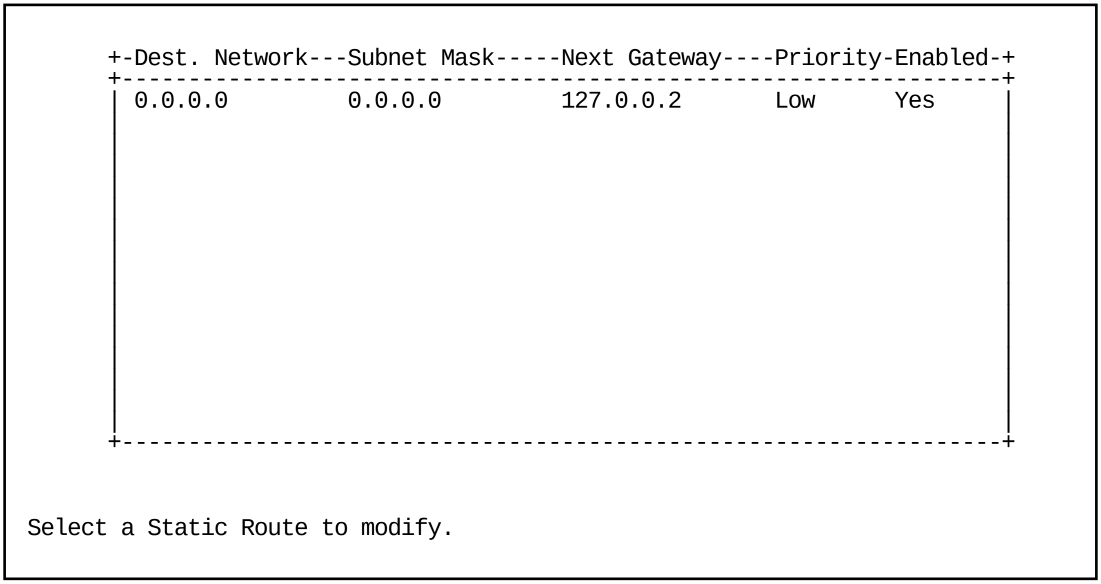
To go to the Static Routes screen, select the **Static Routes** item in the **IP Setup** screen.



```
                             Static Routes

                      Display/Change Static Route...
                      Add Static Route...
                      Delete Static Route...









Configure/View/Delete Static Routes from this and the following Screens.
```

Viewing static routes

To display a view-only table of static routes, select **Display/Change Static Route** in the Static Routes screen.



```
       +-Dest. Network---Subnet Mask-----Next Gateway----Priority-Enabled-+
       +------------------------------------------------------------------+
       | 0.0.0.0         0.0.0.0         127.0.0.2       Low      Yes     |
       |                                                                  |
       |                                                                  |
       |                                                                  |
       |                                                                  |
       |                                                                  |
       |                                                                  |
       |                                                                  |
       +------------------------------------------------------------------+


Select a Static Route to modify.
```

The table has the following columns:

Dest. Network: The network IP address of the destination network.

Subnet Mask: The subnet mask associated with the destination network.

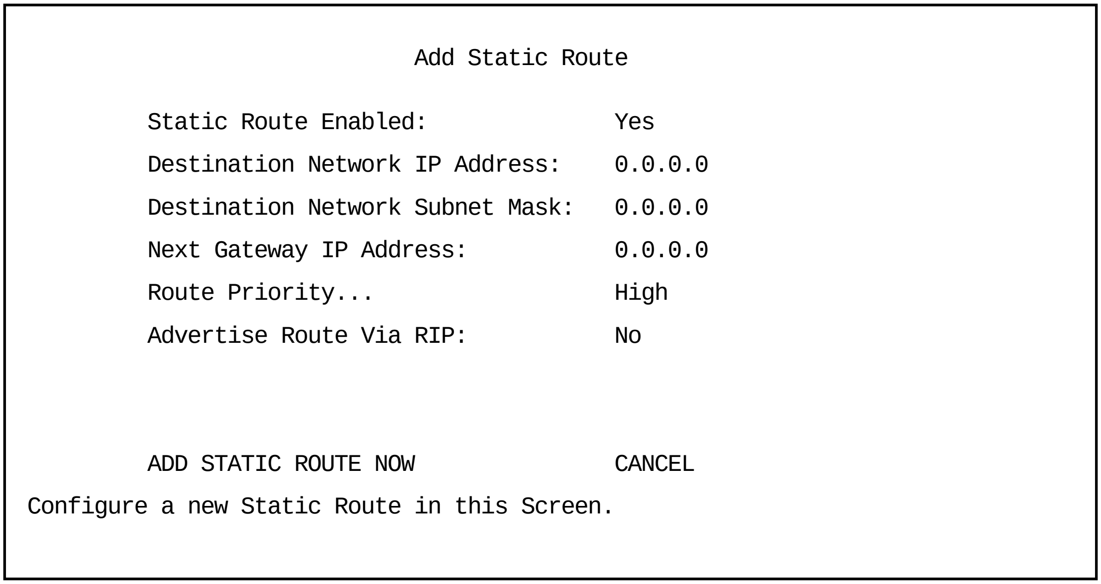
Next Gateway: The IP address of the router that will be used to reach the destination network.

Priority: An indication whether the Netopia R2020 will use the static route when it conflicts with information received from RIP packets.

Enabled: An indication whether the static route should be installed in the IP routing table.

Adding a static route

To add a new static route, select **Add Static Route** in the Static Routes screen and go to the Add Static Route screen.



```
                             Add Static Route

          Static Route Enabled:              Yes
          Destination Network IP Address:    0.0.0.0
          Destination Network Subnet Mask:   0.0.0.0
          Next Gateway IP Address:           0.0.0.0
          Route Priority...                  High
          Advertise Route Via RIP:           No



          ADD STATIC ROUTE NOW               CANCEL
Configure a new Static Route in this Screen.
```

- To install the static route in the IP routing table, select **Static Route Enabled** and toggle it to **Yes**. To remove the static route from the IP routing table, select **Static Route Enabled** and toggle it to **No**.
- Be sure to read the rules on the installation of static routes in the IP routing table. See "Rules of static route installation" on page 10-34.
- Select **Destination Network IP Address** and enter the network IP address of the destination network.
- Select **Destination Network Subnet Mask** and enter the subnet mask used by the destination network.
- Select **Next Gateway IP Address** and enter the IP address for the router that the Netopia R2020 will use to reach the destination network. This router does not necessarily have to be part of the destination network, but it must at least know where to forward packets destined for that network.
- Select **Route Priority** and choose **High** or **Low**. **High** means that the static route takes precedence over RIP information; **Low** means that the RIP information takes precedence over the static route.
- If the static route conflicts with a connection profile, the connection profile will always take precedence.
- To make sure that the static route is known only to the Netopia R2020, select **Advertise Route Via RIP** and toggle it to **No**. To allow other RIP-capable routers to know about the static route, select **Advertise Route Via RIP** and toggle it to **Yes**. When **Advertise Route Via RIP** is toggled to **Yes**, a new item called **RIP Metric** appears below **Advertise Route Via RIP**.

With **RIP Metric** you set the number of routers, from 1 to 15, between the sending router and the destination router. The maximum number of routers on a packet's route is 15. Setting **RIP Metric** to **1** means that a route can involve 15 routers, while setting it to **15** means a route can only involve one router.

- Select **ADD STATIC ROUTE NOW** to save the new static route, or select **CANCEL** to discard it and return to the Static Routes screen.
- Up to 16 static routes can be created, but one is always reserved for the default gateway, which is configured using either Easy Setup or the IP Setup screen in System Configuration.

Modifying a static route

To modify a static route, select **Display/Change Static Route** in the Static Routes screen to display a table of static routes.

Select a static route from the table and go to the Change Static Route screen. The parameters in this screen are the same as the ones in the Add Static Route screen (see "Adding a static route" on page 10-33).

Deleting a static route

To delete a static route, select **Delete Static Route** in the Static Routes screen to display a table of static routes. Select a static route from the table and press Return to delete it. To exit the table without deleting the selected static route, press the Escape key.

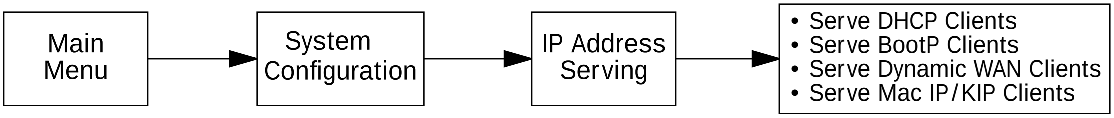
Rules of static route installation

The Netopia R2020 applies certain rules before installing enabled static routes in the IP routing table. An enabled static route will not be installed in the IP routing table if any of the following conditions are true:

- The static route's **Next Gateway IP Address** matches the IP address used by a connection profile or the Netopia R2020's Ethernet port.
- The static route's **Next Gateway IP Address** matches an IP address in the range of IP addresses being distributed by MacIP or DHCP.
- The static route's **Next Gateway IP Address** is determined to be unreachable by the Netopia R2020.
- The static route's route information conflicts with a connection profile's route information.
- The connection profile associated with the static route is set for dial-in connections only, and there is no incoming call connected to that connection profile.
- The connection profile associated with the static route has a disabled dial-on-demand setting, and there is no current connection using that connection profile.

A static route is already installed in the IP routing table will be removed if any of the conditions listed above become true for that static route. However, an enabled static route is automatically reinstalled once the conditions listed above are no longer true for that static route.

IP address serving

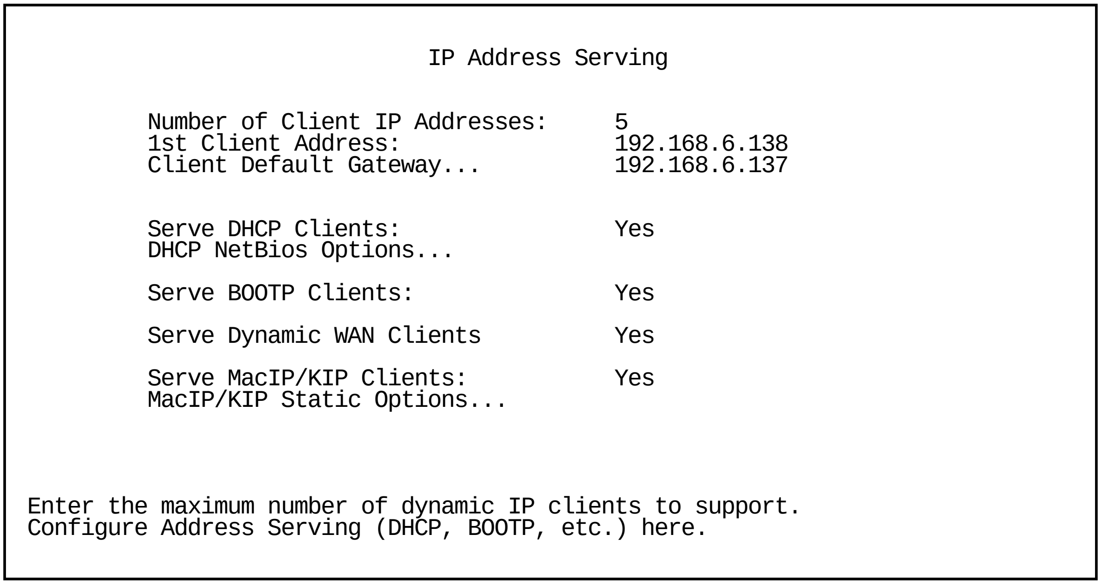


In addition to being a router, the Netopia R2020 is also an IP address server. There are four protocols it can use to distribute IP addresses.

- The first, called **Dynamic Host Configuration Protocol (DHCP)**, is widely supported on PC networks, as well as Apple Macintosh computers using Open Transport and computers using the UNIX operating system. Addresses assigned via DHCP are “leased” or allocated for a short period of time; if a lease is not renewed, the address becomes available for use by another computer. DHCP also allows most of the IP parameters for a computer to be configured by the DHCP server, simplifying setup of each machine.
- The second, called **BOOTP** (also known as Bootstrap Protocol), is the predecessor to DHCP and allows older IP hosts to obtain most of the information that a DHCP client would obtain. However, in contrast, BOOTP address assignments are “permanent” since there is no lease renewal mechanism in BOOTP.
- The third protocol, called **Dynamic WAN**, is part of the PPP/MP suite of wide area protocols used for WAN connections. It allows remote terminal adapters and NAT-enabled routers to be assigned a temporary IP address for the duration of their connection.
- The fourth protocol, called **MacIP**, is used only for computers on AppleTalk networks. MacIP provides a protocol translation (or gateway) function between IP and AppleTalk as well as an IP address assignment mechanism. Like DHCP, MacIP address assignments are normally temporary, although you may also use static IP addresses with MacIP.

Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Netopia R2020, and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

To go to the IP Address Serving screen, select **IP Address Serving** in the System Configuration screen and press Return.



```
                         IP Address Serving

           Number of Client IP Addresses:     5
           1st Client Address:                192.168.6.138
           Client Default Gateway...          192.168.6.137


           Serve DHCP Clients:                Yes
           DHCP NetBios Options...

           Serve BOOTP Clients:               Yes

           Serve Dynamic WAN Clients          Yes

           Serve MacIP/KIP Clients:           Yes
           MacIP/KIP Static Options...



  Enter the maximum number of dynamic IP clients to support.
  Configure Address Serving (DHCP, BOOTP, etc.) here.
```

Follow these steps to configure IP Address Serving:

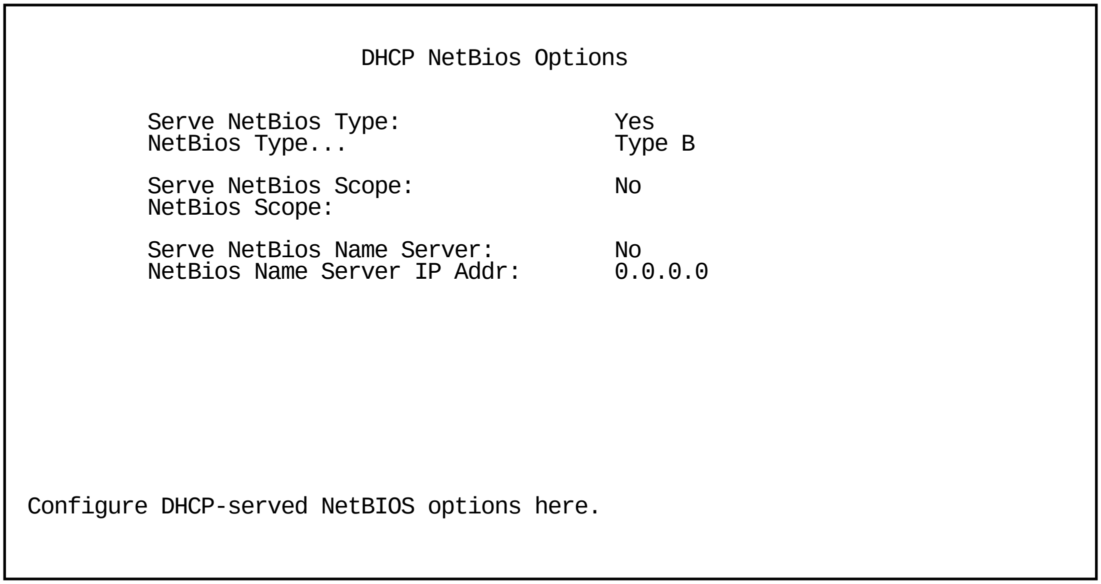
- If you enabled IP Address Serving either by using SmartStart or in Easy Setup, DHCP, BootP clients, Dynamic WAN clients, and MacIP/KIP clients (if you have the AppleTalk kit installed) are automatically enabled.
- Select **Number of Client IP Addresses** and enter the total number of contiguous IP addresses that the Netopia R2020 will distribute to the client machines on your local area network.
- In the screen example shown above, five Client IP addresses have been allocated.
- Select **1st Client Address** and enter the first client IP address that you will allocate to your first client machine. For instance, on your local area network you may first want to figure out what machines are going to be allocated specific static IP addresses so that you can determine the pool of IP addresses that you will be serving addresses from via DHCP, BOOTP, Dynamic WAN, and/or MacIP.
- **Example:** Your ISP has given your Netopia R2020 the IP address 192.168.6.137, with a subnet mask of 255.255.255.248. The subnet mask allocated will give you six IP addresses to use when connecting to the ISP over the Internet (for more information on understanding IP addressing refer to Appendix C, “Understanding IP Addressing.”). Your address range will be from **.137-.143**. In this example you would enter **192.168.6.138** as the 1st client address, as the router itself must have an IP address.
- To enable DHCP, select **Serve DHCP Clients** and toggle it to **Yes**. DHCP serving is automatic when IP Address Serving is enabled.

DHCP NetBIOS Options

If your network uses NetBIOS, you can enable the Netopia R2020 to use DHCP to distribute NetBIOS information.

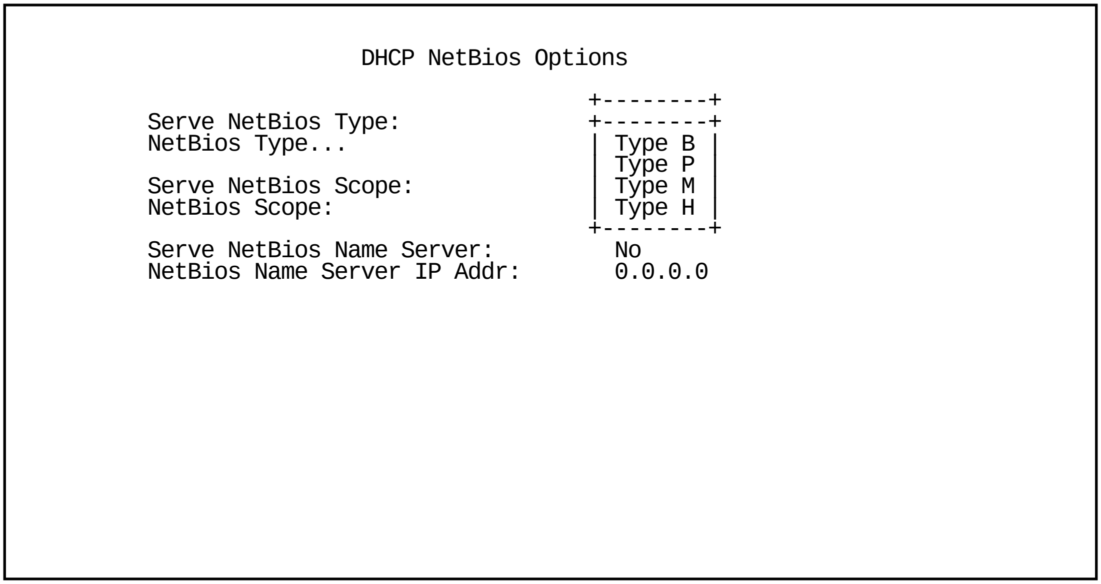
NetBIOS stands for Network Basic Input/Output System. It is a layer of software originally developed by IBM and Sytek to link a network operating system with specific hardware. NetBIOS has been adopted as an industry standard. It offers LAN applications, a variety of “hooks” to carry out inter-application communications and data transfer. Essentially, NetBIOS is a way for application programs to talk to the network. To run an application that works with NetBIOS, a non-IBM network operating system or network interface card must offer a NetBIOS emulator. Many vendors either provide a version of NetBIOS to interface with their hardware or emulate its transport layer communications services in their network products. A NetBIOS emulator is a program provided by NetWare clients that allow workstations to run applications that support IBM’s NetBIOS calls.

- Select **Serve NetBIOS Options** and press Return. The DHCP NetBIOS Options screen appears.



```
                          DHCP NetBios Options

         Serve NetBios Type:                 Yes
         NetBios Type...                     Type B

         Serve NetBios Scope:                No
         NetBios Scope:

         Serve NetBios Name Server:          No
         NetBios Name Server IP Addr:        0.0.0.0






Configure DHCP-served NetBIOS options here.
```

- To serve DHCP clients with the type of NetBIOS used on your network, select **Serve NetBIOS Type** and toggle it to **Yes**.
- From the **NetBIOS Type** pop-up menu, select the type of NetBIOS used on your network.



```
                          DHCP NetBios Options

                                                +--------+
          Serve NetBios Type:                   +--------+
          NetBios Type...                       | Type B |
                                                | Type P |
          Serve NetBios Scope:                  | Type M |
          NetBios Scope:                        | Type H |
                                                +--------+
          Serve NetBios Name Server:              No
          NetBios Name Server IP Addr:            0.0.0.0
```

- To serve DHCP clients with the NetBIOS scope, select **Serve NetBIOS Scope** and toggle it to **Yes**.

  Select **NetBIOS Scope** and enter the scope.

- To serve DHCP clients with the IP address of a NetBIOS name server, select **Serve NetBIOS Name Server** and toggle it to **Yes**.

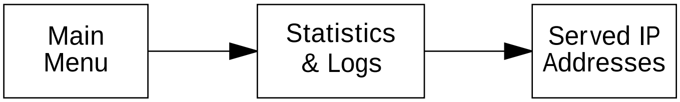
  Select **NetBIOS Name Server IP Address** and enter the IP address for the NetBIOS name server.

  You are now finished setting up DHCP NetBIOS Options. To return to the IP Address Serving screen press the Escape key once.

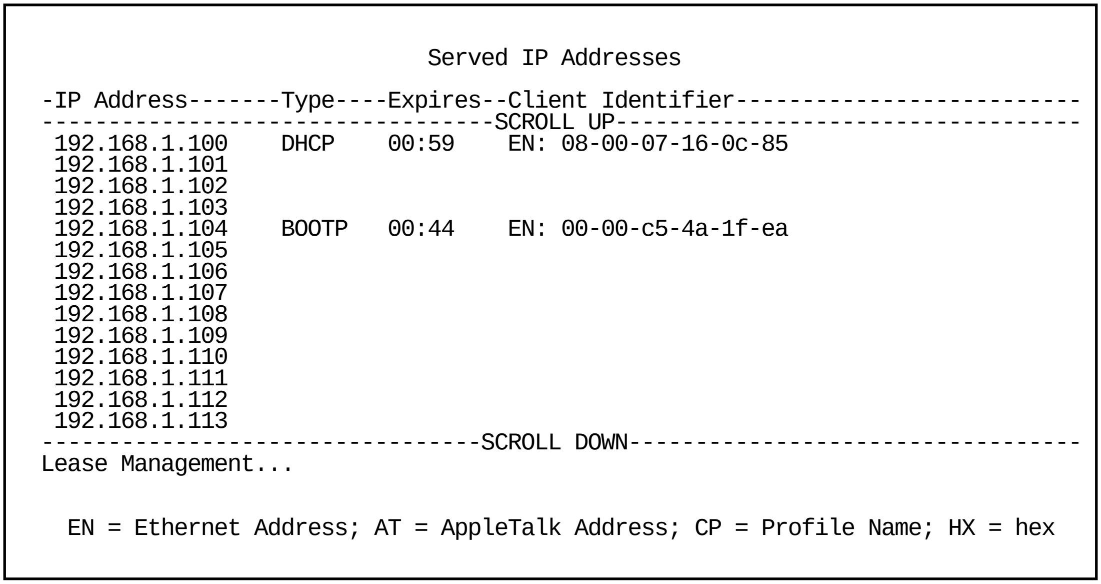
- To enable BootP's address serving capability, select **Serve BOOTP Clients** and toggle to **Yes**.

  Note: Addresses assigned through BOOTP are permanently allocated from the IP Address Serving pool until you release them.

To view all of the IP addresses currently being served by the Netopia R2020, from the Statistics & Logs menu select **Served IP Addresses**.

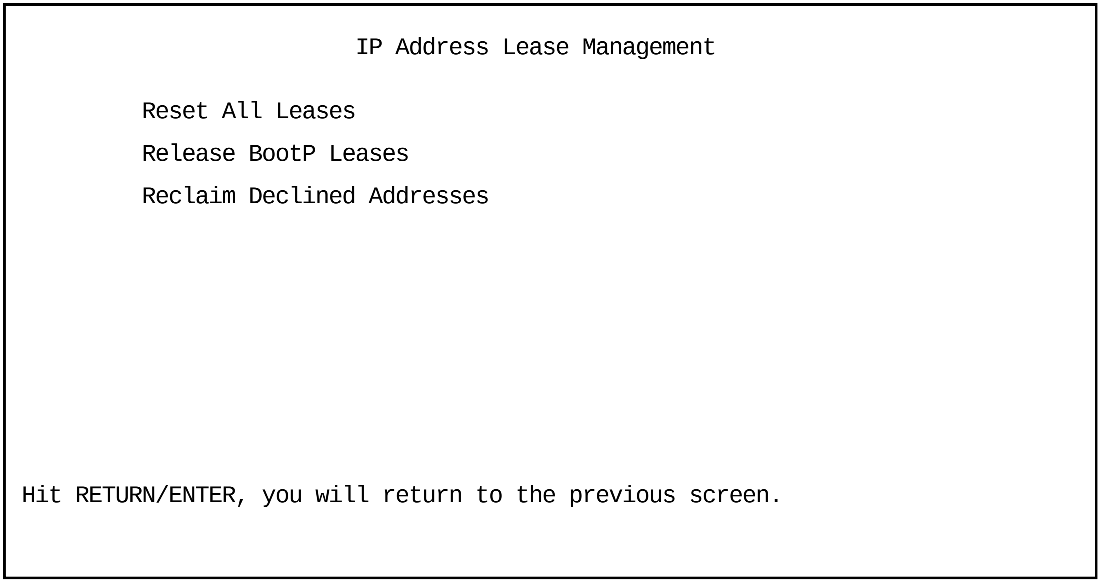


The Served IP Addresses screen appears.



```
                           Served IP Addresses

 -IP Address-------Type----Expires--Client Identifier--------------------------
 ----------------------------------SCROLL UP-----------------------------------
  192.168.1.100    DHCP    00:59    EN: 08-00-07-16-0c-85
  192.168.1.101
  192.168.1.102
  192.168.1.103
  192.168.1.104    BOOTP   00:44    EN: 00-00-c5-4a-1f-ea
  192.168.1.105
  192.168.1.106
  192.168.1.107
  192.168.1.108
  192.168.1.109
  192.168.1.110
  192.168.1.111
  192.168.1.112
  192.168.1.113
 ---------------------------------SCROLL DOWN----------------------------------
 Lease Management...


   EN = Ethernet Address; AT = AppleTalk Address; CP = Profile Name; HX = hex
```

To release these addresses, select **Lease Management**.



```
                        IP Address Lease Management

        Reset All Leases

        Release BootP Leases

        Reclaim Declined Addresses









Hit RETURN/ENTER, you will return to the previous screen.
```

Select **Release BootP Leases** and press Return.

For more lease management information see "Served IP Addresses" on page 13-10.

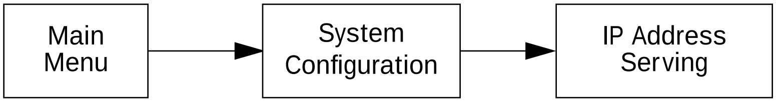
DHCP Relay Agent

The R2020 offers DHCP Relay Agent functionality, as defined in RFC1542. A DHCP relay agent is a computer system or a router that is configured to forward DHCP requests from clients on the LAN to a remote DHCP server, and to pass the replies back to the requesting client systems.

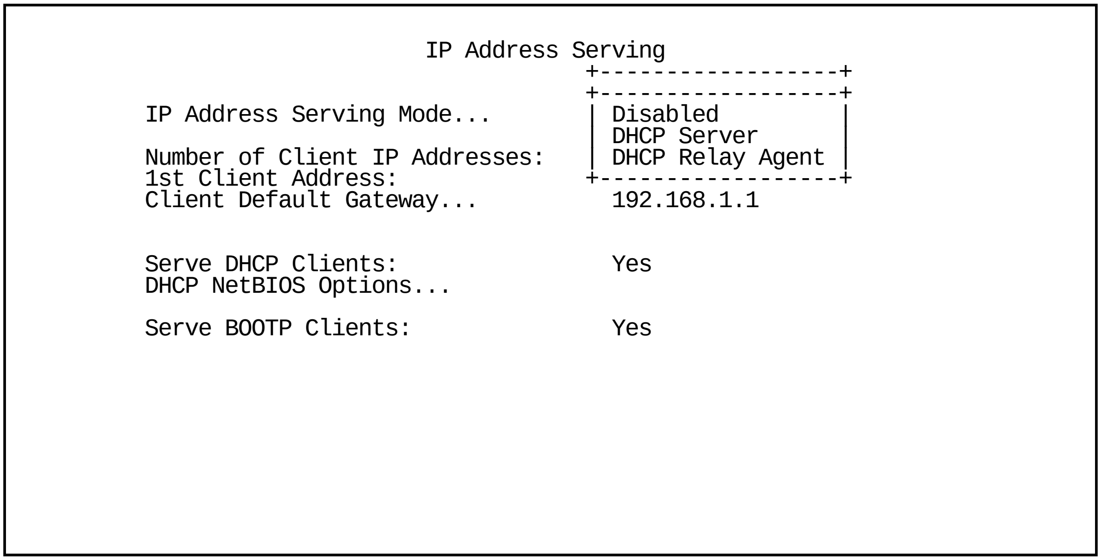
When a DHCP client starts up, it has no IP address, nor does it know the IP address of a DHCP server. Therefore, it uses an IP broadcast to communicate with one or more DHCP servers. These broadcasts are normally limited to the network segment on which the client is located, and do not pass through routers such as the Netopia Router. If the Netopia Router is configured to act as a DHCP server, it will assign the client an address from an address pool configured locally in the Netopia Router and respond to the client's request itself.

However, if the Netopia Router is configured to act as a DHCP relay agent, it does not satisfy the DHCP request itself, but instead forwards the request to one or more remote DHCP servers. These servers process the request, assign an address from an address pool configured on the remote server, and forward the response back to the Netopia Router for delivery back to the client. The agent then sends the response to the client on behalf of the DHCP server. This process is transparent to the client, which doesn't know that it is communicating through an intermediary rather than directly to a local server. Using DHCP relay, it is possible to centralize the configuration information for the host computers at many remote sites at single location, easing the burden of administering configuration management for remote sites.

To configure the Netopia Router to act as a DHCP relay agent, from the Main Menu navigate to the System Configuration menu.



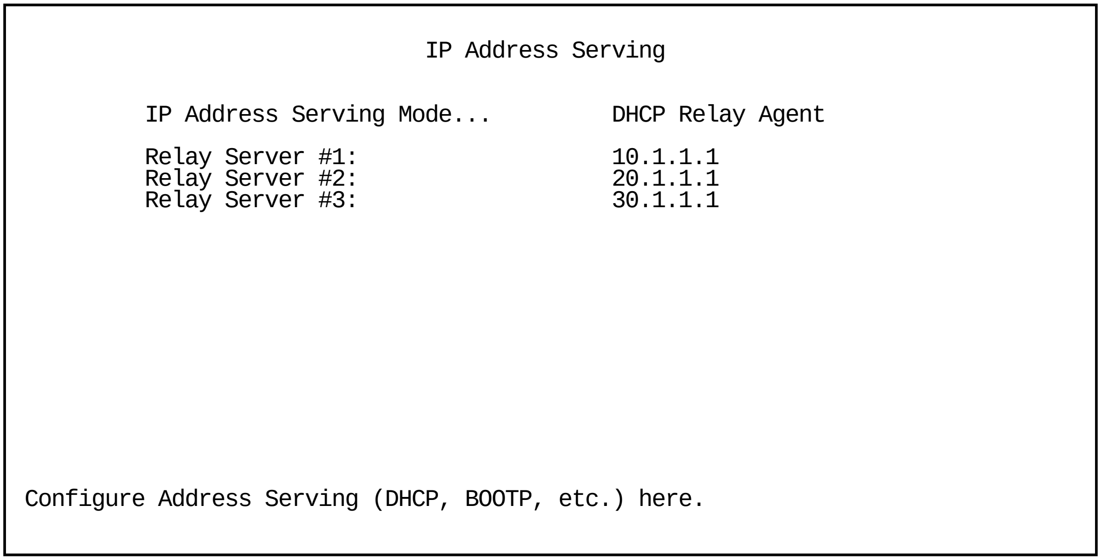
Select **IP Address Serving** and press Return. The IP Address Serving screen appears.



```
                          IP Address Serving
                                        +-------------------+
                                        +-------------------+
IP Address Serving Mode...              | Disabled          |
                                        | DHCP Server       |
Number of Client IP Addresses:          | DHCP Relay Agent  |
1st Client Address:                     +-------------------+
Client Default Gateway...                 192.168.1.1


Serve DHCP Clients:                       Yes
DHCP NetBIOS Options...

Serve BOOTP Clients:                      Yes
```

Select **IP Address Serving Mode**. The pop-up menu offers the choices of Disabled, DHCP Server (the default), and DHCP Relay Agent.

If you select **DHCP Relay Agent** and press Return, the screen changes as shown below.



```
                              IP Address Serving


          IP Address Serving Mode...         DHCP Relay Agent

          Relay Server #1:                   10.1.1.1
          Relay Server #2:                   20.1.1.1
          Relay Server #3:                   30.1.1.1













Configure Address Serving (DHCP, BOOTP, etc.) here.
```

Now you can enter the IP address(es) of your remote DHCP server(s), such as might be located in your company's corporate headquarters. Each time you enter an IP address and press Return, an additional field appears. You can enter up to four DHCP server addresses.

In the example above, DHCP requests from clients on the LAN will be relayed to the DHCP servers at IP addresses 10.1.1.1, 20.1.1.1, and 30.1.1.1.

MacIP (Kip Forwarding) Options

When hosts using AppleTalk (typically those using LocalTalk) are not directly connected to an IP network (usually an Ethernet), they must use a MacIP (AppleTalk-IP) gateway.

The optional Netopia AppleTalk feature enhancement kit provides for this service. A MacIP gateway converts network traffic into the correct format for AppleTalk or IP, depending on the traffic's destination. The MacIP gateway can also distribute IP addresses to AppleTalk computers on the network.

Note: Macintosh computers that have LocalTalk or EtherTalk selected in the MacTCP control panel, or "AppleTalk (MacIP)" selected in the TCP/IP control panel, must use the MacIP gateway to communicate with the Internet or any other IP network. Users should point their MacTCP or TCP/IP control panel to look in the LocalTalk zone for the MacIP server. Macintosh computers that have Ethernet selected in the MacTCP or TCP/IP control panel can do their own AppleTalk-IP conversions.

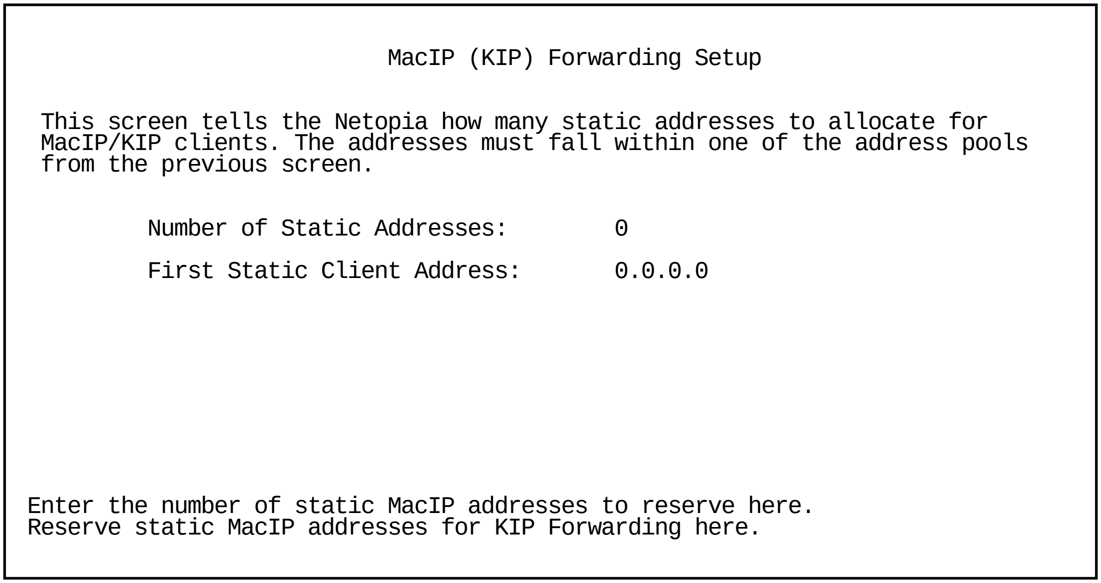
Setting up MacIP involves choosing MacIP dynamic address serving and then configuring that type. KIP forwarding is simply a method for distributing IP addresses to AppleTalk clients.

To go to the MacIP Setup screen, select **MacIP/KIP Clients** in the IP Address Serving screen from the System Configuration menu.

- Select **Serve Mac IP/KIP Clients** and toggle to **Yes**, to enable MacIP/KIP address serving capability. This option is automatically enabled if the AppleTalk kit is installed and IP Address Serving is enabled.

- Select **MacIP/KIP Static Options** and press Return. The MacIP (KIP) Forwarding Setup screen tells the Netopia R2020 how many static addresses to allocate for MacIP/KIP clients. The addresses must fall within the address pool from the previous screen. You will need to enter the number of static MacIP addresses to reserve in this screen.

  Note that the address pool IP range will also be listed for your referral in this screen.



```
                        MacIP (KIP) Forwarding Setup

  This screen tells the Netopia how many static addresses to allocate for
  MacIP/KIP clients. The addresses must fall within one of the address pools
  from the previous screen.

          Number of Static Addresses:        0

          First Static Client Address:       0.0.0.0






 Enter the number of static MacIP addresses to reserve here.
 Reserve static MacIP addresses for KIP Forwarding here.
```

You have finished your IP Setup.

Chapter 11

IPX Setup

Internetwork Packet Exchange (IPX) is the network protocol used by Novell NetWare networks. This chapter shows you how to configure the Netopia R2020 for routing data using IPX. You also learn how to configure the router to serve IPX network addresses.

This section covers the following topics:

IPX Features

The Netopia R2020 supports the following IPX features:

- IPX RIP and SAP
- NetBIOS broadcast packet forwarding (IPX type 20)
- IPX packet filtering definable by source and destination IPX address and socket number, for added security
- IPX SAP filtering to aid in optimizing WAN bandwidth
- Dial-on-demand features:
    - Spoofing of IPX keep-alive, SPX, and server serialization packets
    - Configurable RIP/SAP timers on connection profiles

IPX Definitions

This section defines IPX-related protocols such as RIP, SAP and NetBIOS, in addition to other related terms. See the next section for setup instructions.

Internetwork Packet Exchange (IPX)

IPX is a datagram, connectionless protocol that Novell adapted from Xerox Network System's (XNS) Internet Datagram Protocol (IDP). IPX is dynamically routed, and the routing architecture works by "learning" network addressing automatically.

IPX address

An IPX address consists of a network number, a node number, and a socket number. An IPX network number is composed of eight hexadecimal digits. The network number must be the same for all nodes on a particular physical network segment. The node number is composed of twelve hexadecimal digits and is usually the hardware address of the interface card. The node number must be unique inside the particular IPX network. Socket numbers correspond to the particular service being accessed.

Socket

A socket in IPX is the equivalent of a port in TCP/IP. Sockets route packets to different processes within a single node. Novell has reserved several sockets for use in the NetWare environment:

Field Value	Packet Type	Description
00h	Unknown Packet Type	Used for all packets not classified by any other type
01h	Routing Information Packet	Unused for RIP packets
04h	Service Advertising Packet	Used for SAP packets
05h	Sequenced Packet	Used for SPX packets
11h	NetWare Core Protocol Packet	Used for NCP packets
14h	Propagated Packet	Used for Novell NetBIOS

Routing Information Protocol (RIP)

RIP, which was also derived from XNS, is a protocol that allows for the bidirectional transfer of routing tables and provides timing information (ticks), so that the fastest route to a destination can be determined. IPX routers use RIP to create and dynamically maintain databases of internetwork routing information. See the last section in this chapter for more information on routing tables.

Service Advertising Protocol (SAP)

SAP is a protocol that provides servers and routers with a method to exchange service information. Using SAP, servers advertise their services and addresses. Routers collect this information to dynamically update their routing tables and share it with other routers. These broadcasts keep all routers on the internetwork synchronized and provide real-time information on accessible servers on the internetwork.

The following is a list of common SAP server types:

Unknown	0000h
Print Queue	0003h
File Server	0004h
Job Server	0005h
Print Server	0007h
Archive Server	0009h
Remote Bridge Server	0024h
Advertising Print Server	0047h
Reserved Up To	8000h

NetBIOS

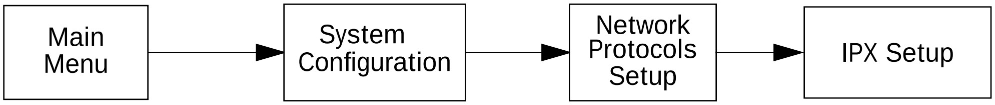
NetBIOS is a protocol that performs tasks related to the Transport and Session layers of the OSI model. It can operate over IPX, using a special broadcast packet known as “IPX Packet type 20” to communicate with IPX NetBIOS servers.

IPX Spoofing

The Netopia R2020 has several IPX features designed to restrict the traffic on the dial-up link when the unit is not sending or receiving IPX data. When the link is idle and a user is logged into a Novell server, the server will send “keep alive” packets to ensure the user is still there. If the link is idle, the “keep alive” packets will be sent back to the server by the locally connected Netopia R2020 as though they came back from the user without bringing up the dial-up link.

Similarly, “SPX keep alive” packets are treated in this manner. IPX RIP, and SAP messages will not be sent if the link is down. Together these features enable the user to remain connected to a Novell server or SPX peer without bringing up the dial-up link, except to send and receive actual user data.

IPX setup

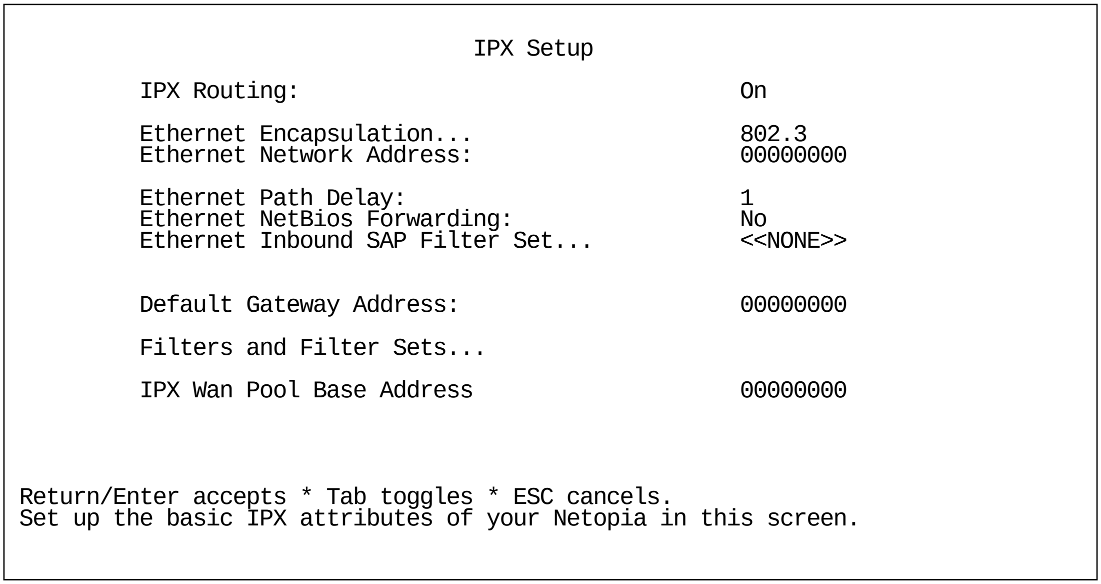


The IPX Setup screen is where you configure the Ethernet side of the Netopia R2020. The information you enter here controls how the Router routes IPX traffic.

Consult your network administrator for the IPX setup information you will need before changing any of the settings in this screen. Changes made in this screen will take effect only after the Netopia R2020 is reset.

To go to the IPX Setup screen, from the Main Menu select System Configuration and then select **Network Protocols Setup** and then select **IPX Setup**.

Note: If you have completed Easy Setup, the information you have already entered will appear in the IP Setup options screen.



```
                              IPX Setup

          IPX Routing:                                  On

          Ethernet Encapsulation...                     802.3
          Ethernet Network Address:                     00000000

          Ethernet Path Delay:                          1
          Ethernet NetBios Forwarding:                  No
          Ethernet Inbound SAP Filter Set...            <<NONE>>


          Default Gateway Address:                      00000000

          Filters and Filter Sets...

          IPX Wan Pool Base Address                     00000000



Return/Enter accepts * Tab toggles * ESC cancels.
Set up the basic IPX attributes of your Netopia in this screen.
```

1. To enable IPX routing, select **IPX Routing**, toggle it to **On**, and press Return.
2. To change Ethernet encapsulation from the commonly used 802.3 standard, select **Ethernet Encapsulation** and choose a different encapsulation method.
3. Select **Ethernet Network Address** and enter the network address of the IPX network connected to the Netopia R2020's Ethernet port.

   Note: If the Ethernet network address is set to zero, the Router will attempt to learn the address from any configured IPX device on the Ethernet network or from the remote IPX network when a call is established.
4. To change the default path delay, select **Ethernet Path Delay** and enter a value (in ticks). This value is used to determine the port cost of using the Ethernet port in IPX RIP calculations.
5. To enable NetBIOS packet forwarding, select **Ethernet NetBIOS Forwarding** and toggle it to **Yes**. This parameter will determine whether "IPX Packet type 20" packets are forwarded on the Ethernet interface. These packets are used by NetBIOS and some other applications.
6. Select **Ethernet Inbound SAP Filter Set** to filter incoming IPX SAP advertisements on the Ethernet. By attaching an incoming SAP filter on the Ethernet, you can restrict the number of SAP entries learned on a large IPX network to only those required by remote users connecting to the Netopia R2020. An Ethernet SAP filter *must* be used with networks that have so many servers advertised that the Netopia R2020 would otherwise exhaust its internal memory storing server entries.

   To attach a SAP filter set, first define the filter set using the **Filters and Filter Sets** option (see step 8 below). Then select the filter set from the **Ethernet Incoming SAP Filter Set** pop-up menu. To detach the filter set, select **Detach Filter Set**.

7. Select **Default Gateway Address**, and enter the network address of the IPX network to which all packets of unknown destination address should be routed.

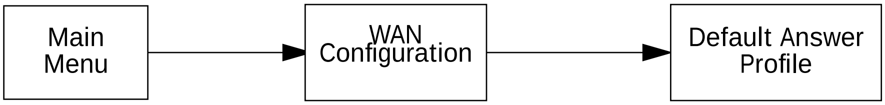
   Note: The Default Gateway Address is usually set up to match the IPX Address in your network Connection Profile.

8. To configure filters and filter sets, select **Filters and Filter Sets** and go to the IPX filters and filter sets screens. For information on how to configure IPX filters and filter sets, see "IPX filters" on page 14-21.

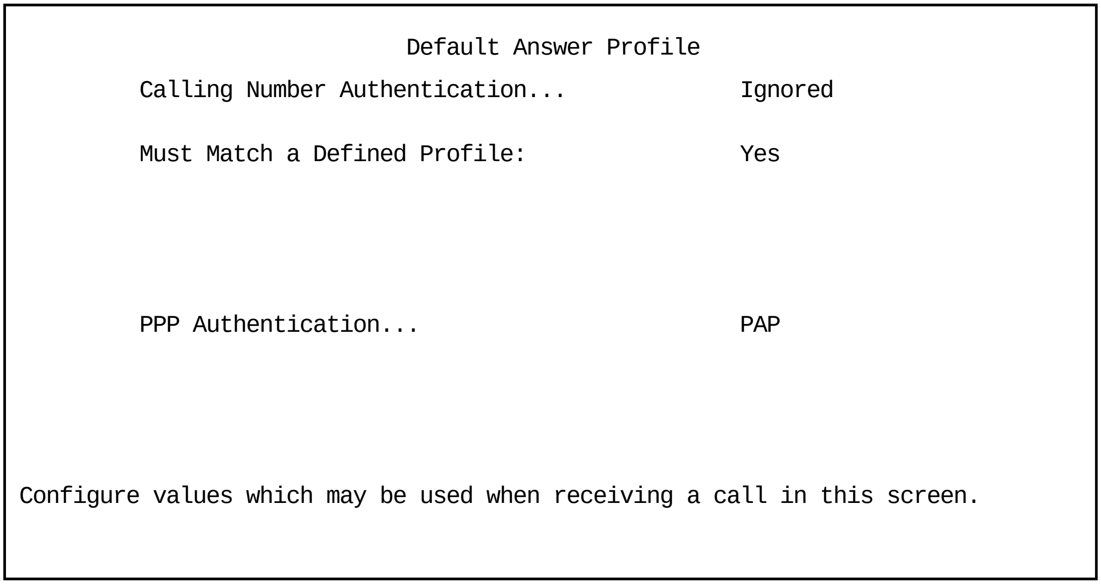
9. Select **IPX Wan Pool Base Address** and enter the first IPX network address to be allocated to requesting IPX WAN clients. The base address you enter must not conflict with other IPX networks assigned to your IPX internet.

IPX in the answer profile

The answer profile can be configured to accept calls from remote IPX networks. To configure the answer profile to accept calls from remote IPX networks, from the **WAN Configuration** menu go to the Default Answer Profile screen.



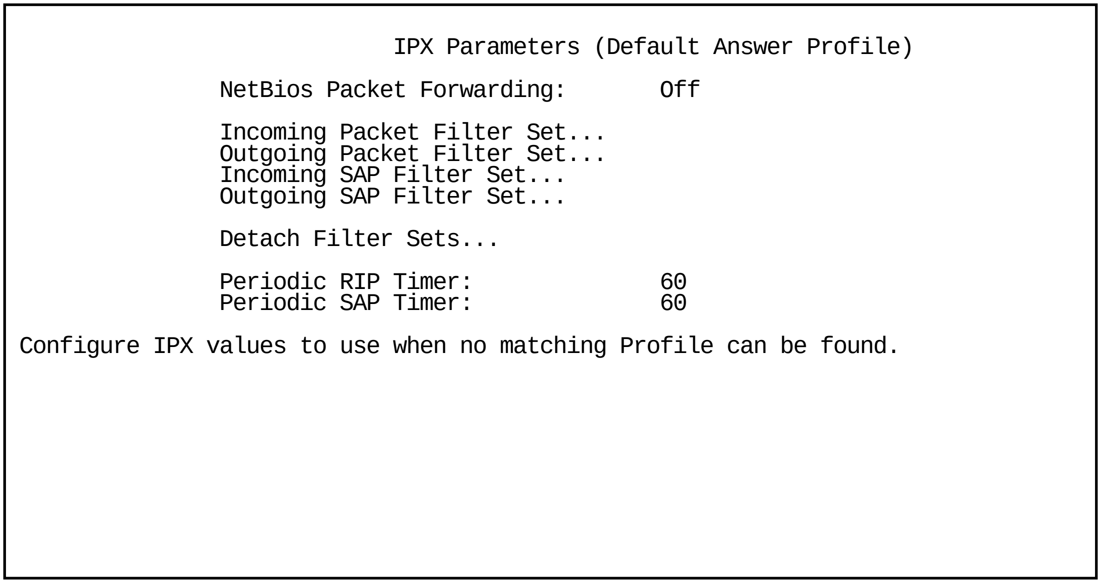
Note: The Default Answer Profile screen varies according to configuration.



```
                          Default Answer Profile
          Calling Number Authentication...               Ignored

          Must Match a Defined Profile:                  Yes




          PPP Authentication...                          PAP





 Configure values which may be used when receiving a call in this screen.
```

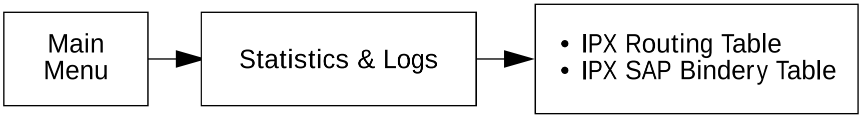
To enable IPX routing in the answer profile, select **IPX Enabled** and toggle it to **Yes**. When **IPX Enabled** is set to **Yes**, the item **IPX Parameters** appears below it.

To configure IPX routing in the answer profile, select **IPX Parameters** and go to the IPX Parameters (Default Answer Profile) screen. The items in this screen are similar to the IPX Profile Parameters items of the same name (see page 11-5).



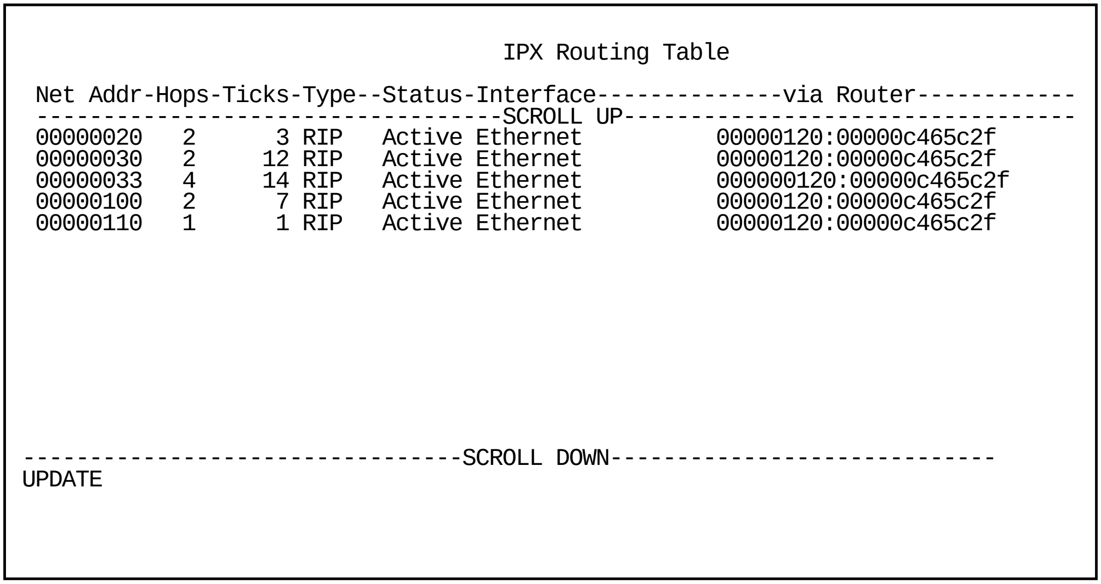
```
                            IPX Parameters (Default Answer Profile)

               NetBios Packet Forwarding:       Off

               Incoming Packet Filter Set...
               Outgoing Packet Filter Set...
               Incoming SAP Filter Set...
               Outgoing SAP Filter Set...

               Detach Filter Sets...

               Periodic RIP Timer:              60
               Periodic SAP Timer:              60

Configure IPX values to use when no matching Profile can be found.
```

IPX routing tables



IPX routing tables provide information on current IPX routes and services.

To go to the IPX Routing Table screen, select **IPX Routing Table** in the Routing Tables screen. This table shows detailed information about current IPX network routes.



```
                                    IPX Routing Table

  Net Addr-Hops-Ticks-Type--Status-Interface--------------via Router------------
  -----------------------------------SCROLL UP----------------------------------
  00000020   2      3 RIP   Active Ethernet          00000120:00000c465c2f
  00000030   2     12 RIP   Active Ethernet          00000120:00000c465c2f
  00000033   4     14 RIP   Active Ethernet          000000120:00000c465c2f
  00000100   2      7 RIP   Active Ethernet          00000120:00000c465c2f
  00000110   1      1 RIP   Active Ethernet          00000120:00000c465c2f







 ---------------------------------SCROLL DOWN-----------------------------
 UPDATE
```

To go to the IPX SAP Bindery Table screen, select **IPX SAP Bindery Table** in the Routing Tables screen. This table shows detailed information about available IPX services and their location.

Chapter 12

AppleTalk Setup

This chapter discusses the concept of AppleTalk routing and how to configure AppleTalk Setup for a Netopia R2020 with the AppleTalk kit installed.

AppleTalk support is available as a separate kit for the Netopia R2020 Dual Analog Router. Skip this chapter if you do not have the AppleTalk kit.

This section covers the following topics:

Note: All changes to AppleTalk options require a restart to take effect.

AppleTalk networks

A **network** is a communication system that connects computers to share information using **network services**, such as electronic mail, print spoolers, and file servers. Information is transferred over a cabling system or WAN using a common set of **protocols**. You can think of the cabling system as an organization of cities, streets, and buildings and the protocols as the method of sending letters or packages, as illustrated on the following pages. A **cable** is the physical medium (for example, twisted pair or coaxial) over which information travels from one device to another.

AppleTalk protocol

AppleTalk is a protocol set for local area networks developed by Apple Computer. While initially applied to the **LocalTalk** cabling system for connecting Macintosh computers and LaserWriters, it has been expanded to use other cabling systems, such as Ethernet, as well as the dial-up telephone networks and packet switching systems. LocalTalk was originally known as the AppleTalk Personal Network system.

Each computer or peripheral device (printer, client, file server) connected to a network is called a **node** and has a unique **node address**, which can be any number from 1 to 254. Whenever you open the Chooser or any application that communicates with other computers on your network, your application compiles a list of all node names and addresses. All you see are the names -- for example, “Paul’sMac,” “TechSportsWriter,” or “2nd Floor AppleShare” -- but your application also knows the node addresses of all these devices.

When you send information, commands, or requests to a printer, server, or another workstation, your application formats the information into units known as **packets**. It then attaches the correct address to the packets and sends them to the AppleTalk software on your computer, which forwards the packets across the network. Packets also include a return address, so the receiver will know where to reply.

If the cabling of your network were a street system, then a node address would correspond to a building's street address. Node addresses are not permanent. Each AppleTalk device determines its node address at startup. Although a Macintosh that is starting up will try to use its previous address, the address will often be different upon restart. This **dynamic node addressing** scheme prevents conflicts when devices are moved between networks and simplifies the administrative tasks of a network. If you have only one network, the node address alone is all the information AppleTalk needs to send a packet from one computer to another.

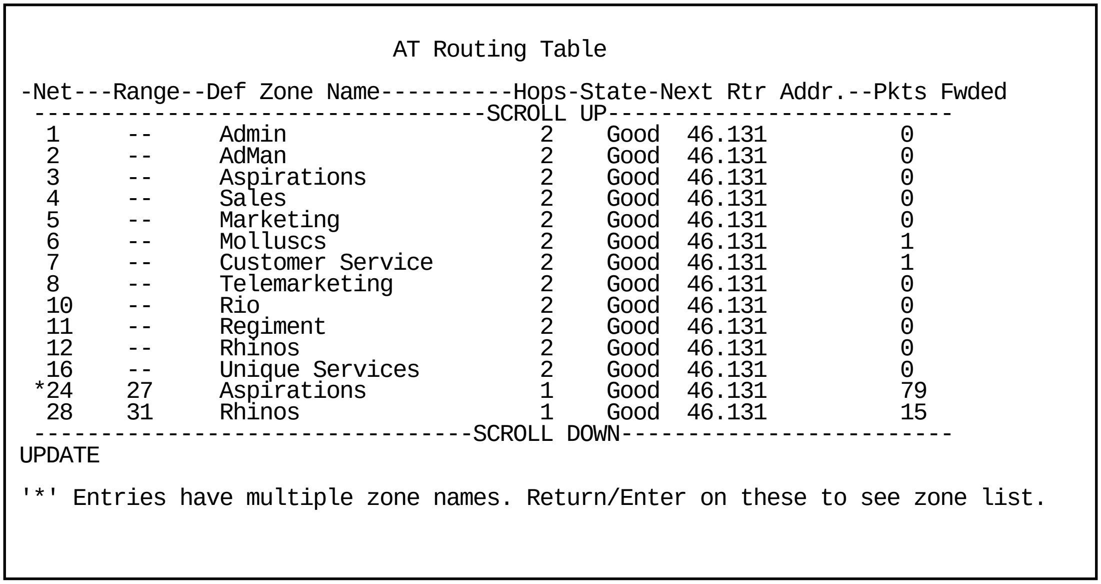
However, networks can be connected together through **routers**, such as the Netopia R2020, into an **internetwork** (often shortened to **internet**). Because devices on different networks can have duplicate node numbers, AppleTalk tells them apart according to an additional part of their addresses: the **network number**.

The Netopia R2020 assigns a unique network number to each member network. In terms of the city street metaphor, the network number is similar to the name of the street. Putting a network number together with a node number fully specifies the address of a node on an internet.

To make the services on an internet manageable, groups of devices on a network can be grouped into zones. When this is done, selecting a network service (server, etc.) includes choosing a zone from which the service can be selected. Like network numbers, **zone names** are assigned by routers.

A **routing table** is maintained by each AppleTalk router. The table serves as a map of the internet, specifying the path and distance, in hops, between its router and other networks. The routing table is used to determine whether a router will forward a data packet and, if so, to which network.

You can use the information in the AppleTalk routing table to observe and diagnose the Netopia R2020's current connections to other AppleTalk routers. To go to the AT Routing Table screen from the Netopia R2020's console, select **Statistics & Logs** from the Main Menu and then select **AppleTalk Routing Table**.



```
                            AT Routing Table

-Net---Range--Def Zone Name----------Hops-State-Next Rtr Addr.--Pkts Fwded
 ----------------------------------SCROLL UP-------------------------
  1     --     Admin                  2    Good  46.131         0
  2     --     AdMan                  2    Good  46.131         0
  3     --     Aspirations            2    Good  46.131         0
  4     --     Sales                  2    Good  46.131         0
  5     --     Marketing              2    Good  46.131         0
  6     --     Molluscs               2    Good  46.131         1
  7     --     Customer Service       2    Good  46.131         1
  8     --     Telemarketing          2    Good  46.131         0
  10    --     Rio                    2    Good  46.131         0
  11    --     Regiment               2    Good  46.131         0
  12    --     Rhinos                 2    Good  46.131         0
  16    --     Unique Services        2    Good  46.131         0
 *24    27     Aspirations            1    Good  46.131         79
  28    31     Rhinos                 1    Good  46.131         15
 ---------------------------------SCROLL DOWN------------------------
UPDATE

'*' Entries have multiple zone names. Return/Enter on these to see zone list.
```

A router has multiple communications ports and is capable of forwarding information to other routers and devices on the internet. The router performs packet forwarding, network and device address maintenance, and other administrative functions required by the AppleTalk protocols.

MacIP

When Macintosh computers encapsulate TCP/IP packets in AppleTalk, either because they are on LocalTalk or they are on EtherTalk for administrative reasons, they must use the services of a MacIP gateway. This gateway converts network traffic into the correct format for AppleTalk or IP, depending on the traffic's destination. Setting up MacIP involves enabling the feature and optionally setting up a range of addresses to be static.

See Chapter 10, "Multiple Network Address Translation and IP Setup," for more information on how to set up MacIP and other IP addressing schemes.

AURP

AppleTalk Update-Based Routing Protocol (AURP) allows AppleTalk networks to communicate across an IP network. Your local AppleTalk networks (connected to the Netopia R2020) can exchange data with remote AppleTalk networks that are also connected to an AURP-capable router.

When two networks using AppleTalk communicate with each other through a network based on the Internet Protocol, they are said to be tunneling through the IP network. The Netopia R2020 uses AURP to allow your AppleTalk network to tunnel to designated AppleTalk partner networks, as well as to accept connections from remote AppleTalk networks tunneling to your AppleTalk LAN.

Routers and seeding

To configure AppleTalk networks, you must understand the concept of **seeding**. Seeding is the process by which routers (or more specifically, router ports) agree on what routing information is valid. AppleTalk routers that have been reset, for example, must decide what zones and network numbers are valid before they begin routing. In this case, a router may use the information it has stored, or use information it receives from another router, depending on how it has been configured.

To help ensure agreement between routers on a network, a **seed router** is configured with the correct information, and other routers obtain their information from that router when they are turned on or reset.

Routers commonly use one of three types of seeding procedures: hard seeding, soft seeding, and non-seeding.

Hard seeding: When a router that uses hard seeding is turned on or reset, it requests network number and zone name information from any existing routers on the networks it will serve. If no other routers reply, the router uses the network numbers and zone names specified in its own configuration. If other routers reply, and their information matches the router's own configuration information, the result is the same—the router uses the values in its own configuration. However, if other routers provide network numbers or zone names that conflict with those in the router's configuration, the router disables any of its own ports for which there are conflicts.

Soft seeding: When a router that uses soft seeding is turned on or reset, it requests network number and zone name information from any existing routers on the networks it will serve. If no other routers reply, the router uses the network numbers and zone names specified in its own configuration. If other routers reply, the router uses the information they provide, regardless of whether or not there are conflicts between the information received and its configured information. Once a soft- or hard seeding router begins to route, it can serve as a seed router, providing network number and zone name information to other routers upon request. The default state of the Netopia R2020's AppleTalk ports is soft seeding.

Non-seeding: When a router using non-seeding is turned on or reset, it requests network number and zone name information from any existing routers on the networks it will serve. For any network where no other routers reply, the non-seeding router will not have any active ports until the next reset.

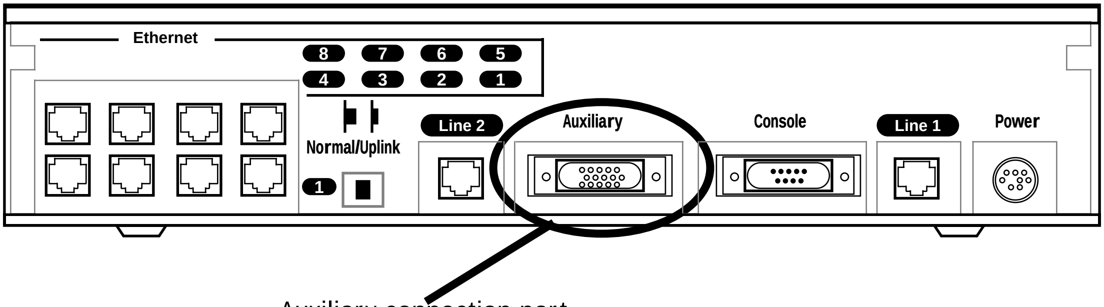
You should set the Netopia R2020’s seeding action to work best in your particular network environment. These scenarios may guide you in deciding how to set the router’s seeding:

- If the Netopia R2020 is the only router on your network, you must set it to either hard seeding or soft seeding. The default is soft seeding.
- If there is another active router on your network, and you want that router to configure the Netopia R2020’s EtherTalk or LocalTalk parameters, you can set the Netopia R2020 to non-seeding.
- If there is another active router on your network, you could set the Netopia R2020 to be soft seeding if you are unsure that the second router would always be available to configure the Netopia R2020’s EtherTalk or LocalTalk parameters.
- If you want the Netopia R2020 to configure the EtherTalk or LocalTalk parameters of other routers on your network, you must set it to hard seeding. In this case, the other routers must be soft seeding or non-seeding, and the Netopia R2020 must already be active when those other routers are rebooted.
- If you want the Netopia R2020 and all other routers on your network to use only their own configurations, set the Netopia R2020 and all other routers to hard seeding. In this case, any router (including the Netopia R2020) that is rebooted will not begin routing if it detects a routing conflict between itself and any other router. This last scenario could be useful for detecting and locating routing errors on your network.

Installing AppleTalk

The AppleTalk kit consists of hardware and firmware components that you enable on your router in order to connect an AppleTalk network. The LocalTalk connector supplied in the AppleTalk feature expansion kit cable connects to the Auxiliary port on the Netopia R2020.

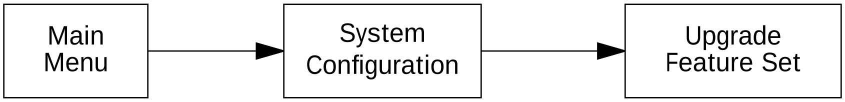
Netopia R2020 back panel



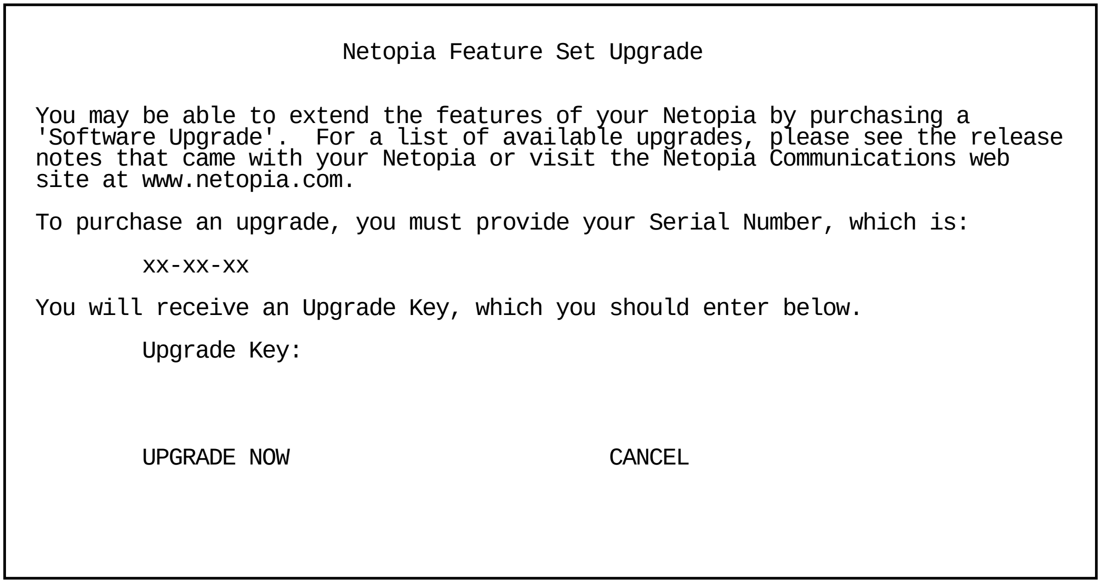
Auxiliary connection port
HD-15 (female)

You then enable AppleTalk routing through the Console-based management screens.

To install the AppleTalk features from the Main Menu, go to System Configuration and select **Upgrade Feature Set**.



The **Netopia Feature Set Upgrade** screen appears.



```
                         Netopia Feature Set Upgrade

You may be able to extend the features of your Netopia by purchasing a
'Software Upgrade'.  For a list of available upgrades, please see the release
notes that came with your Netopia or visit the Netopia Communications web
site at www.netopia.com.

To purchase an upgrade, you must provide your Serial Number, which is:

        xx-xx-xx

You will receive an Upgrade Key, which you should enter below.

        Upgrade Key:



        UPGRADE NOW                        CANCEL
```

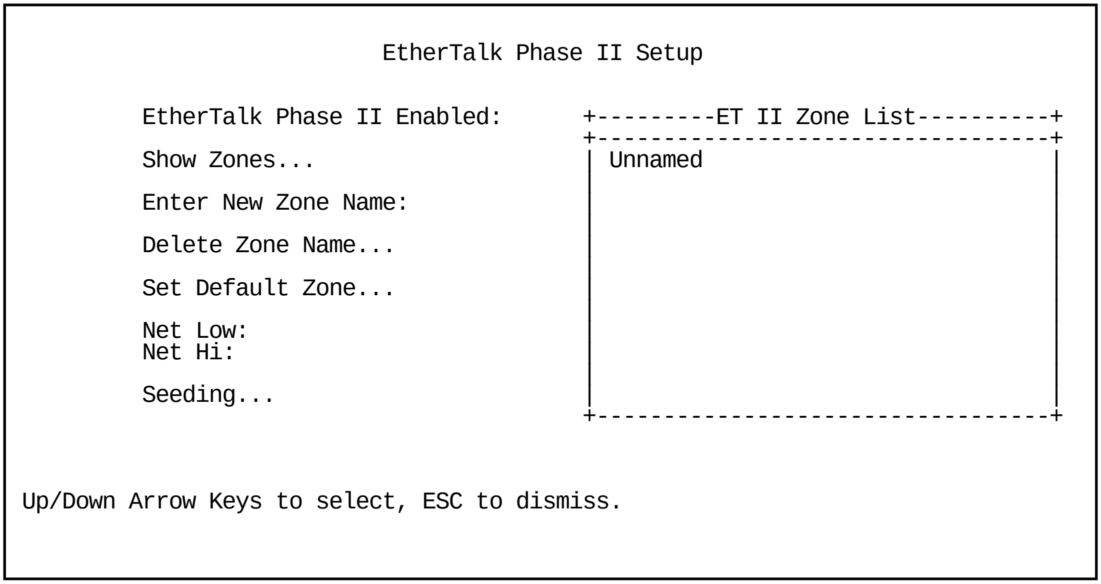
Follow the instructions to enable AppleTalk on your router. Once AppleTalk is enabled, you can configure your network as described in the following sections.

Configuring AppleTalk

AppleTalk setup for Netopia R2020s consists of configuring EtherTalk, LocalTalk, and AURP.

EtherTalk Setup

To go to the EtherTalk Setup options screen, select **Network Protocols Setup** and then select **AppleTalk Setup** in the System Configuration screen. Select **EtherTalk Phase II Setup** and press Return.



```
                            EtherTalk Phase II Setup


          EtherTalk Phase II Enabled:      +---------ET II Zone List----------+
                                           +----------------------------------+
          Show Zones...                    | Unnamed                          |
                                           |                                  |
          Enter New Zone Name:             |                                  |
                                           |                                  |
          Delete Zone Name...              |                                  |
                                           |                                  |
          Set Default Zone...              |                                  |
                                           |                                  |
          Net Low:                         |                                  |
          Net Hi:                          |                                  |
                                           |                                  |
          Seeding...                       |                                  |
                                           +----------------------------------+



 Up/Down Arrow Keys to select, ESC to dismiss.
```

- If you are using EtherTalk Phase II on the Ethernet network connected to Netopia R2020, select **EtherTalk Phase II Enabled** and toggle it to **On**.
- To view the zones available to EtherTalk Phase II, select **Show Zones** and press Return. You can dismiss the list of zones by pressing the Return or Escape key.
- Select **Enter New Zone Name** to enter a new zone name.

  Note: Your EtherTalk network number and zone name must match the values in use on the EtherTalk network.

  If another router is already present on the EtherTalk network that you will be connecting to the Netopia R2020, use the zone names and network numbers used by that router for that EtherTalk network. Otherwise, your EtherTalk network may experience routing conflicts. The Netopia R2020 supports creating up to 32 zone names.

  As an alternative, you can set EtherTalk seeding to soft seeding and let the Netopia R2020 receive the zone name and network number from the other router.
- To remove zones from the list, select **Delete Zone Name** and press Return to see the zones list. Use the Up and Down Arrow keys to select the zone to delete. Press the Return key to delete it and exit the list. Press the Escape key to exit the list without deleting any zones.
- Select **Set Default Zone** to choose a different default zone. This is the zone where the Netopia R2020's

EtherTalk Phase II port is visible to other AppleTalk nodes. The default zone is also where new AppleTalk nodes will appear. If you do not set a default zone, the first zone you create will be the default zone.

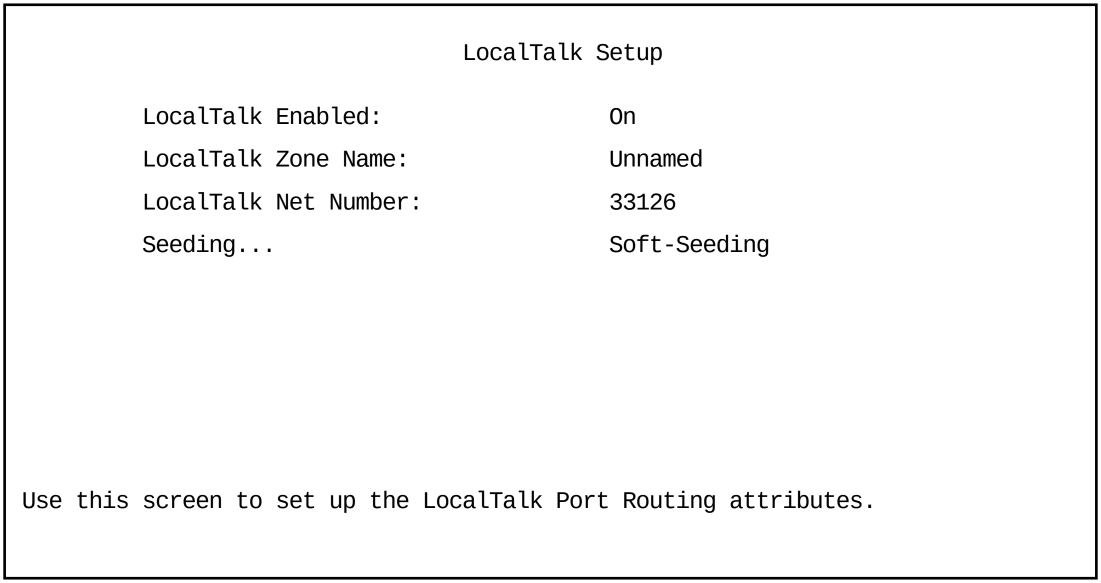
- You can also set the range of EtherTalk Phase II network numbers. Select **Net Low** and enter the lower limit of the network number range. Select **Net High** and enter the upper limit of the range.
- Select the **Seeding** pop-up menu and choose the seeding method for the Netopia R2020 to use (see "Routers and seeding" on page 12-3).

You have finished configuring EtherTalk Phase II.

LocalTalk Setup

Note: For instructions on making the physical connections for LocalTalk, see "Connecting to a LocalTalk network" on page 4-5.

Select **LocalTalk Setup** in the AppleTalk Setup screen and press Return to the LocalTalk Routing Setup screen.



```
                              LocalTalk Setup

          LocalTalk Enabled:                  On
          LocalTalk Zone Name:                Unnamed
          LocalTalk Net Number:               33126
          Seeding...                          Soft-Seeding








 Use this screen to set up the LocalTalk Port Routing attributes.
```

- If you are using LocalTalk with the Netopia R2020, select **LocalTalk Enabled** and make sure LocalTalk is set to **On,** which is the default.

Note: Since the LocalTalk connector attaches to the Auxiliary port on the router, that port will no longer be available for a third external modem.

- Select **LocalTalk Zone Name** and enter a new or existing zone name.

  Note: Your LocalTalk network may already have a zone and network number in place. For the Netopia R2020's LocalTalk port to be part of your LocalTalk network, it must have a network number and zone name that matches the values in use on the LocalTalk network.

  If another router is already present on the LocalTalk network that you will be connecting to the Netopia R2020, use the zone name and network number used by that router for that LocalTalk network. Otherwise, your LocalTalk network may experience routing conflicts.

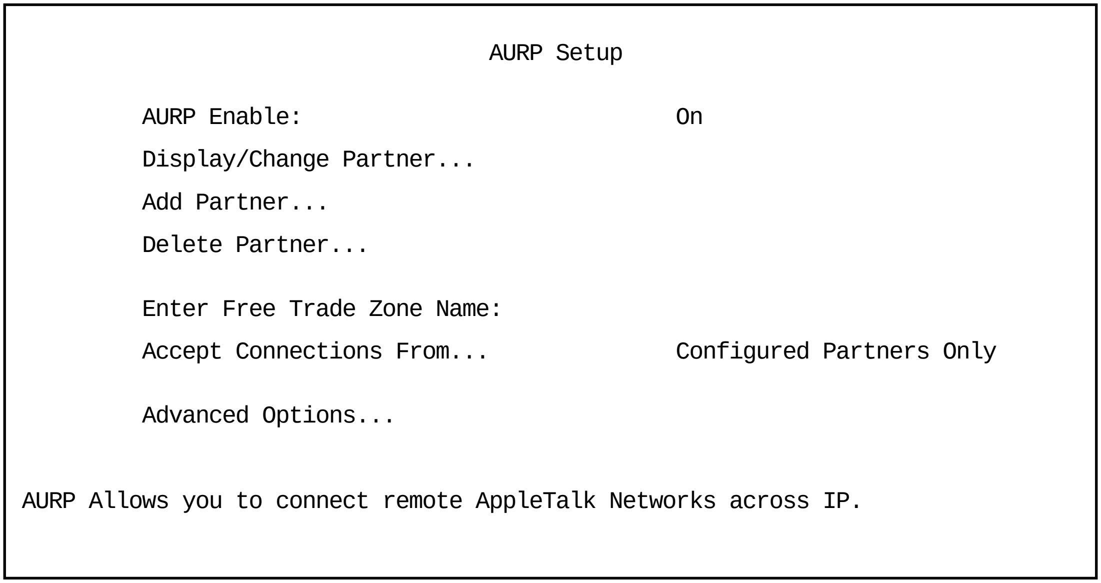
As an alternative, you can set LocalTalk seeding to soft seeding and let the Netopia R2020 receive the zone name and network number from the other router.

- Select **LocalTalk Network Number** and enter the desired network number.
- Select **Seeding.** From the pop-up menu, choose the type of seeding for the Netopia R2020's LocalTalk port to use (see "Routers and seeding" on page 12-3).

You have finished configuring LocalTalk.

AURP setup

To set up AURP, select AppleTalk Setup from the Network Protocols screen. Select **AURP Setup** and press Return.



```
                                AURP Setup

          AURP Enable:                              On
          Display/Change Partner...
          Add Partner...
          Delete Partner...

          Enter Free Trade Zone Name:
          Accept Connections From...                Configured Partners Only

          Advanced Options...


 AURP Allows you to connect remote AppleTalk Networks across IP.
```

- To activate AURP and enable connections to and from AURP partners, select **AURP Enable** and toggle it to **On**.

Viewing AURP partners

- To see a table of existing AURP partners, select **Display / Show Partners** and press Return.

  Note: The Netopia R2020 can define a total of 32 AURP partners.

AURP Free Trade Zone

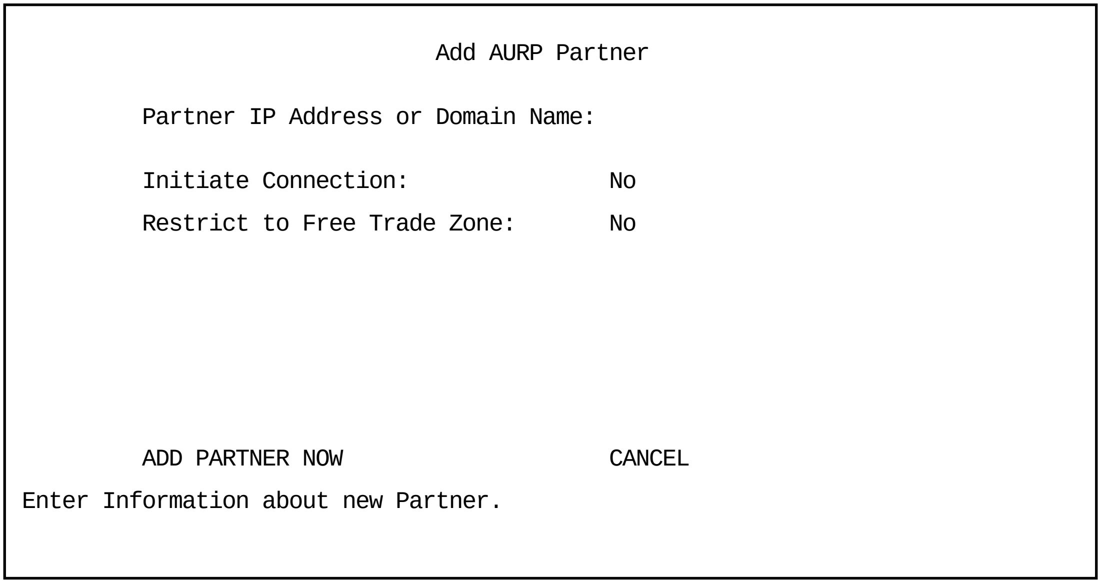
The Free Trade Zone is an AURP security feature. It allows the Netopia administrator to specify a single AppleTalk zone that will be the only one visible to the remote side for partners that have this option enabled.

Example:

Site A has an AURP tunnel to site B. Both sides have multiple zones defined on the EtherTalk port and a unique zone on their LocalTalk ports. If side A has indicated one of its EtherTalk zones is the Free Trade Zone and has opted to use the Free Trade Zone option for its tunnel to B, then only this Free Trade Zone will show up on side B and only those machines or services in the Free Trade Zone will be accessible to side B. All of side A will be able to see all of side B.

Adding an AURP partner

- To add a new AURP partner, select **Add Partner** and press Return to go to the Add AURP Partner screen.



```
                         Add AURP Partner

     Partner IP Address or Domain Name:

     Initiate Connection:               No

     Restrict to Free Trade Zone:       No






     ADD PARTNER NOW                    CANCEL

Enter Information about new Partner.
```

- Select **Partner IP Address or Domain Name** and enter the new AURP partner’s IP address. If you do not know the remote network’s IP address, enter its domain name. Domain names are the Internet addresses favored by people (for example, chagall.arts.edu). Domain names are matched to the IP addresses actually used by IP routers (for example, 163.7.8.202).
- To initiate a connection with an AURP partner, select **Initiate Connection** and toggle it to **Yes**. This will open a connection to the remote AppleTalk network after rebooting.
- You can choose to restrict this partner to the Free Trade Zone by toggling **Restrict to Free Trade Zone** to **Yes**. See “AURP Free Trade Zone” on page 12-8 for more information.
- To add the new AURP partner, select **ADD PARTNER NOW**. To discard the new AURP partner, select **CANCEL**.

Modifying an AURP partner

- To modify an AURP partner, select **Display/Change Partner** in the AURP Setup screen and press Return to display a table of existing partners.

  Use the Up and Down Arrow keys to select a partner, then press Return to go to the Change AURP Partner screen.

Deleting an AURP partner

- To delete an AURP partner, select **Delete Partner** in the AURP Setup screen and press Return to display a table of existing partners.

  Use the Up and Down Arrow keys to select an AURP partner, then press Return to delete it. Press the Escape key to exit without deleting a partner.

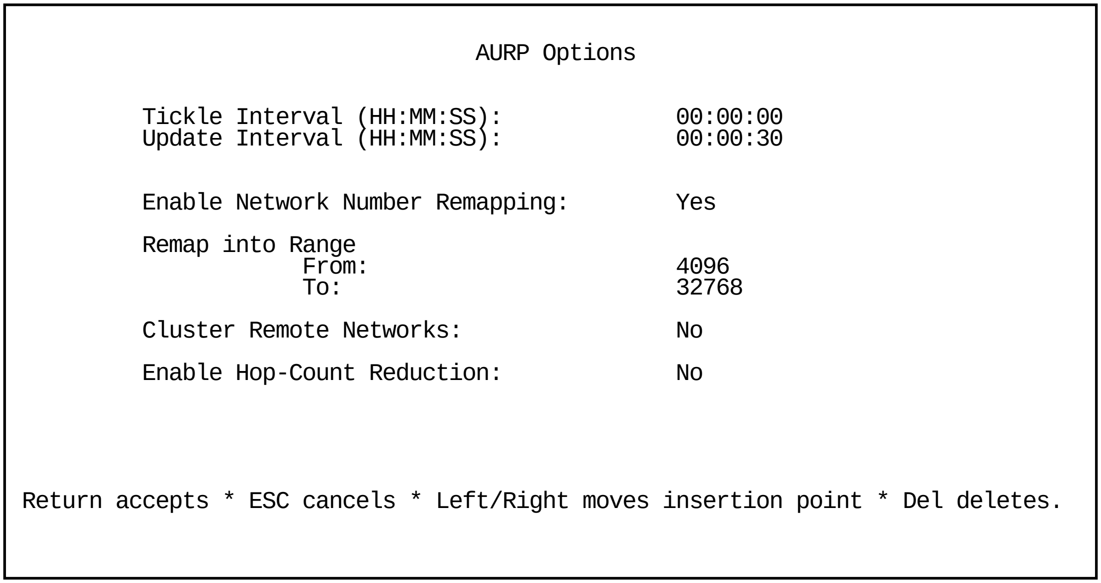
Receiving AURP connections

- To control the acceptance of incoming AURP tunnels, select **Accept Connections From** and choose **Anyone** or **Configured Partners Only** from the pop-up menu. If you choose **Anyone**, all incoming AURP connections will be accepted.

  The more secure option is **Configured Partners Only**, which only accepts connections from recognized AURP partners (the ones you have set up).

Configuring AURP Options

In the AURP Setup screen, Select **AURP Options** and go to the AURP Options screen. Using AURP can cause a problem when two networks, one local and one remote, have the same network number. This may cause network routing ambiguities than can result in routing errors.



```
                              AURP Options

          Tickle Interval (HH:MM:SS):            00:00:00
          Update Interval (HH:MM:SS):            00:00:30

          Enable Network Number Remapping:       Yes

          Remap into Range
                      From:                      4096
                      To:                        32768

          Cluster Remote Networks:               No

          Enable Hop-Count Reduction:            No



 Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
```

- Select **Tickle Pkt Rqst Interval (HH:MM:SS)** and set the timer to indicate how often a tickle or ‘are you still there’ packet will be sent to the remote AppleTalk Network.

  The AURP tickle timer is a parameter that you can set anywhere between 0 and 100 hours. This parameter tells the AURP partners when to send out an AURP tickle packet. If this value is set to 0, the Netopia R2020 will never send out a tickle packet. Tickle packets verify that the remote router is working. The minimum tickle interval is 90 seconds. The maximum tickle interval setting is 99:59:59 (100 hours), which is the recommendation for small networks.

Raising the tickle packet interval does not ensure that the AURP tunnel is dropped or not brought up. If any application on the local network generates AppleTalk traffic destined for the network at the remote end of the AURP tunnel, the tunnel remains up. For example, if a host on the local network connects to a host on the remote network using remote access software, the AURP tunnel remains up. The AURP tunnel also remains up if a local user selects the Chooser and uses an AppleTalk service that involves a remote zone, such as mounting a remote AppleShare volume.

- In many AppleTalk internets, individual AppleTalk networks come and go. Routers are designed to notify each other at the end of their **Update Interval** every time there's such a change in the network topology. This will cause the Netopia's WAN link to be brought up. You can opt to minimize what may be unnecessary calls by changing the Update Interval value to some larger value. At the end of this time window if there has been a local AppleTalk network change the Netopia R2020 will call any remote AURP partner and forward the new network information.
- To enable network number remapping, select **Enable Network Number Remapping** and toggle it to **Yes**.

  You should enable network number remapping if you plan on using AURP when connecting to unknown AppleTalk networks. for example when "Accept Connections from Anyone" is enabled. With remapping, the Netopia R2020 will substitute network numbers not used by your network for the numbers of other remote networks. These safe remappings will only be used by local routers on your network; remote routers will not be aware of the remapping.

  When network number remapping is enabled, you *must* choose a safe range of network numbers as a destination for the remapping. A safe range of network numbers does not intersect your local AppleTalk network's range of network numbers.
- To choose a destination range for the remapping, select **From** under **Remap into Range** and enter a starting value. Then select **To** and enter an ending value. Make sure the range you choose is large enough to accommodate all expected incoming AURP network numbers.
- To improve the efficiency of remapping network numbers into a safe range, select **Cluster Remote Networks** and toggle it to **Yes**. This setting takes any number of remote networks being remapped and causes them to be remapped into a continuous range.
- To override the AppleTalk maximum limit of 15 hops, select **Enable Hop-Count Reduction** and toggle it to **Yes**. Hosts on a local AppleTalk network will then "see" AppleTalk destinations across the IP tunnel as being only one hop away.

  AppleTalk allows a packet up to 15 hops (going through 15 AppleTalk routers) to reach its destination. Packets that must reach destinations more than 15 hops away will not succeed, therefore tunneling from one large AppleTalk network to another could exceed that limit. In such a case, hop count reduction enables full network to network communication.

You have finished configuring AURP.

Chapter 13

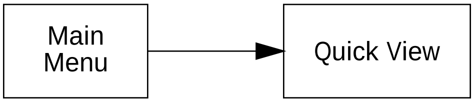
Monitoring Tools

This chapter discusses the Netopia R2020's device and network monitoring tools. These tools can provide statistical information, report on current network status, record events, and help in diagnosing and locating problems.

This section covers the following topics:

Quick View status overview

You can get a useful, overall status report from the Netopia R2020 in the Quick View screen. To go to the Quick View screen, select **Quick View** in the Main Menu.

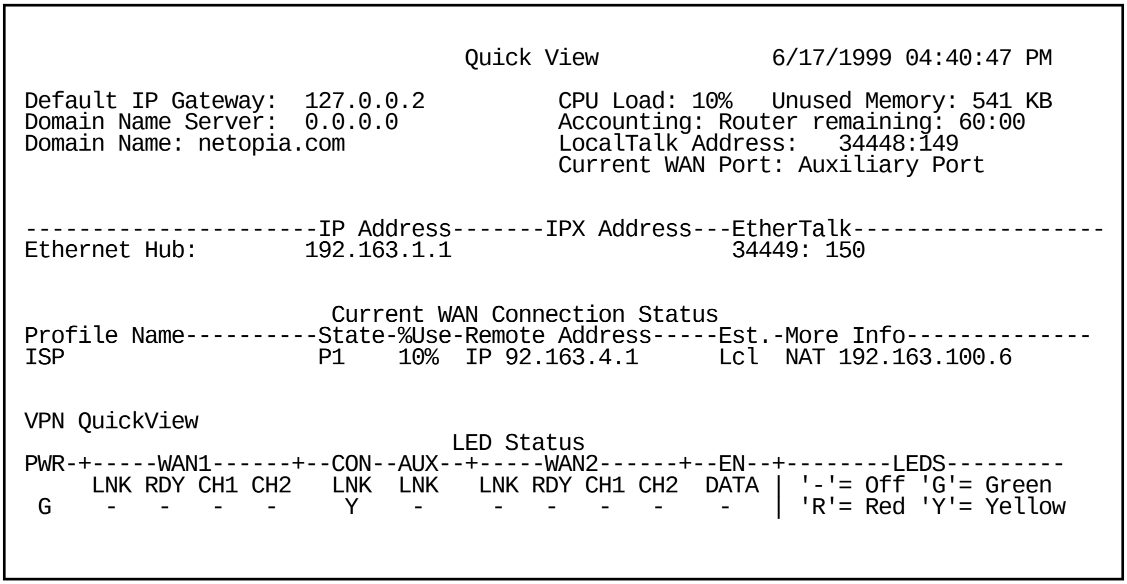


The Quick View screen has three status sections:

- General status
- Current WAN Connection Status
- LED Status

The status sections vary according to the interface of your Netopia R2020.

General Status



```
                                 Quick View             6/17/1999 04:40:47 PM

Default IP Gateway:  127.0.0.2          CPU Load: 10%   Unused Memory: 541 KB
Domain Name Server:  0.0.0.0            Accounting: Router remaining: 60:00
Domain Name: netopia.com                LocalTalk Address:   34448:149
                                        Current WAN Port: Auxiliary Port


----------------------IP Address-------IPX Address---EtherTalk-------------------
Ethernet Hub:        192.163.1.1                     34449: 150


                       Current WAN Connection Status
Profile Name----------State-%Use-Remote Address-----Est.-More Info--------------
ISP                   P1    10%  IP 92.163.4.1      Lcl  NAT 192.163.100.6


VPN QuickView
                                LED Status
PWR-+-----WAN1------+--CON--AUX--+-----WAN2------+--EN--+--------LEDS---------
     LNK RDY CH1 CH2   LNK  LNK   LNK RDY CH1 CH2  DATA | '-'= Off 'G'= Green
 G    -   -   -   -     Y    -     -   -   -   -    -   | 'R'= Red 'Y'= Yellow
```

Current Date: The current date; this can be set with the Date and Time utility (see "Date and Time" on page 7-11).

Default IP Gateway: The router's default gateway, which may be either manually configured or learned via DHCP. This is the value you assigned in the Default IP Gateway field on page 6-5. If you are using the router's defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as your default gateway, it is shown here.

CPU Load: Percentage of the system's resources being used by all current transmissions.

Unused Memory: The total remaining system memory available for use.

Domain Name Server: If you are using the router's defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as your default gateway, it is shown here.

Accounting: Shows whether you have enabled or disabled the call accounting features.

Domain Name: the domain name you have assigned, typically the name of your ISP

Current WAN Port: Indicates which port is in use.

IP Address: The Netopia R2020's IP address, entered in the IP Setup screen.

IPX Address: The Netopia R2020's IPX address, entered in the IPX Setup screen.

EtherTalk Address: The Netopia R2020's AppleTalk address on its EtherTalk Phase II interface, entered in the EtherTalk Phase II Setup screen (only if the optional AppleTalk feature set is installed).

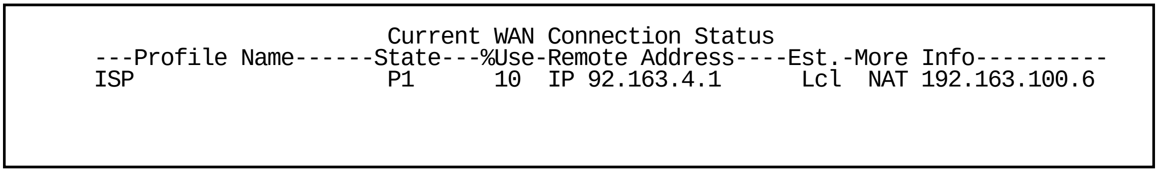
LocalTalk Address: The Netopia R2020's AppleTalk address on its LocalTalk interface, entered in the LocalTalk Setup screen (only if the optional AppleTalk feature set is installed).

VPN QuickView. Access point for the VPN QuickView status monitoring screen. See "VPN QuickView" on page 9-9.

Current Status

The current status section is a table showing the current status of the WAN. For example:

WAN Status



```
                          Current WAN Connection Status
    ---Profile Name------State---%Use-Remote Address----Est.-More Info----------
    ISP                   P1      10  IP 92.163.4.1      Lcl  NAT 192.163.100.6
```

Profile Name: Lists the name of the connection profile being used, if any.

State: Lists the ports in use for this connection.

%Use: Indicates the average percent utilization of the maximum capacity of the channels in use for the connection.

Remote Address: Shows the IP address of the connected remote router if the connection is using IP. Otherwise, shows the IPX address of the connected remote router, if using IPX. If the directory number was entered in the WAN configuration (see "Specifying telephone connections" on page 8-1) it shows the called directory number if locally originated, otherwise the calling directory number (if available).

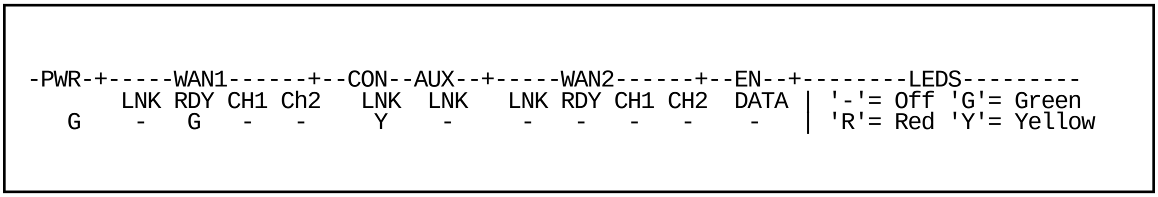
Est: Indicates whether the connection was locally ("Lcl") or remotely ("Rmt") established.

More Info: Indicates, in order of priority, the NAT address in use for this connection, the IPX address in use (if IP is also in use), or the ISDN caller identification (if available).

Status lights

This section shows the current real-time status of the Netopia R2020's status lights (LEDs). It is useful for remotely monitoring the router's status. The Quick View screen's arrangement of LEDs corresponds to the physical arrangement of LEDs on the router.

LED Status



```
-PWR-+-----WAN1------+--CON--AUX--+-----WAN2------+--EN--+--------LEDS---------
       LNK RDY CH1 Ch2   LNK  LNK   LNK RDY CH1 CH2  DATA | '-'= Off 'G'= Green
   G    -   G   -   -     Y    -     -   -   -   -    -   | 'R'= Red 'Y'= Yellow
```

Each LED representation can report one of four states:

–: A dash means the LED is off.

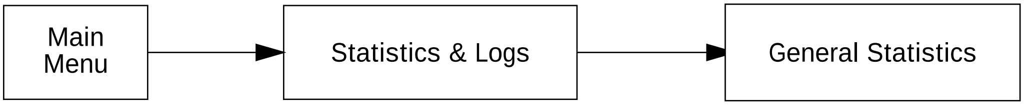
R: The letter "R" means the LED is red.

G: The letter "G" means the LED is green.

Y: The letter "Y" means the LED is yellow.

The section "Netopia R2020 Dual Analog Router Status Lights" on page 2-6 describes the meanings of the colors for each LED.

Statistics & Logs



When you are troubleshooting your Netopia R2020, the Statistics screens provide insight into the recent event activities of the Router.

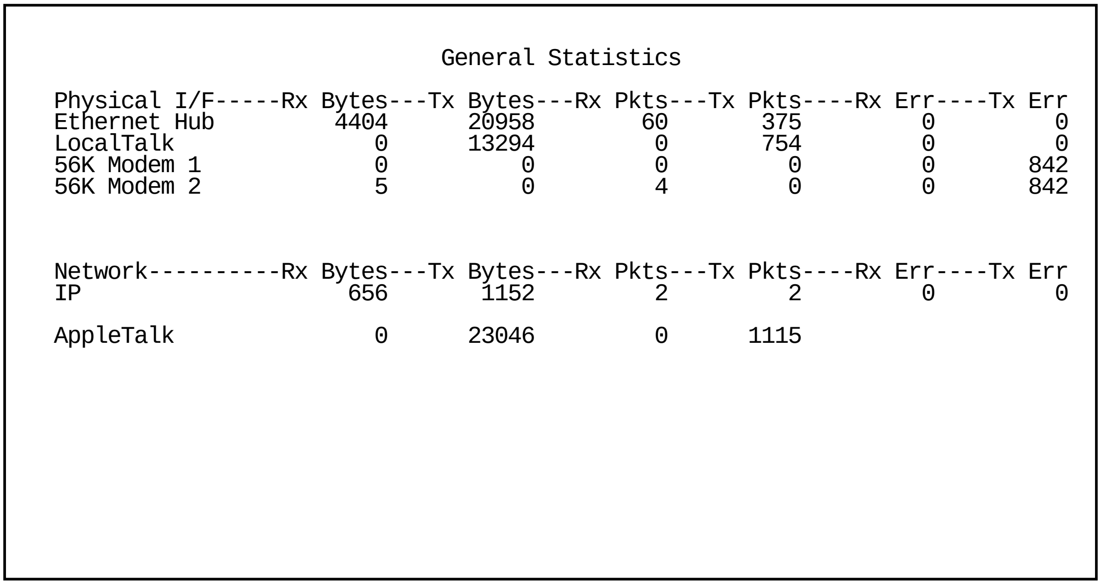
From the Main Menu go to **Statistics & Logs** and select one of the options described in the sections below.

General Statistics

To go to the General Statistics screen, select **General Statistics** in the Statistics & Logs screen.

General Statistics

General Statistics screen



```
                              General Statistics

   Physical I/F-----Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts----Rx Err----Tx Err
   Ethernet Hub         4404      20958         60       375         0         0
   LocalTalk               0      13294          0       754         0         0
   56K Modem 1             0          0          0         0         0       842
   56K Modem 2             5          0          4         0         0       842


   Network----------Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts----Rx Err----Tx Err
   IP                    656       1152          2         2         0         0

   AppleTalk               0      23046          0      1115
```

General Statistics displays information about data traffic on the Netopia R2020’s data ports. This information is useful for monitoring and troubleshooting your LAN.

The left side of the screen lists total packets received and total packets transmitted for the following protocols:

- IP (IP packets on the Ethernet)
- IPX (IPX packets on the Ethernet) if IPX is enabled
- ET II (AppleTalk packets on Ethernet, using EtherTalk Phase II) if the optional AppleTalk feature set is installed
- LT (LocalTalk on the PhoneNET) if the optional AppleTalk feature set is installed

The right side of the table lists the total number of occurrences of each of five types of communication statistics:

EN Rx Packets: The number of Ethernet packets received.

EN Rx Errors: The number of bad Ethernet packets received.

EN Collisions: An error occurring when Ethernet packets are transmitted simultaneously by nodes on the LAN.

WAN Connection Statistics

The WAN Connection Statistics give the following information about each channel of the point-to-point interface:

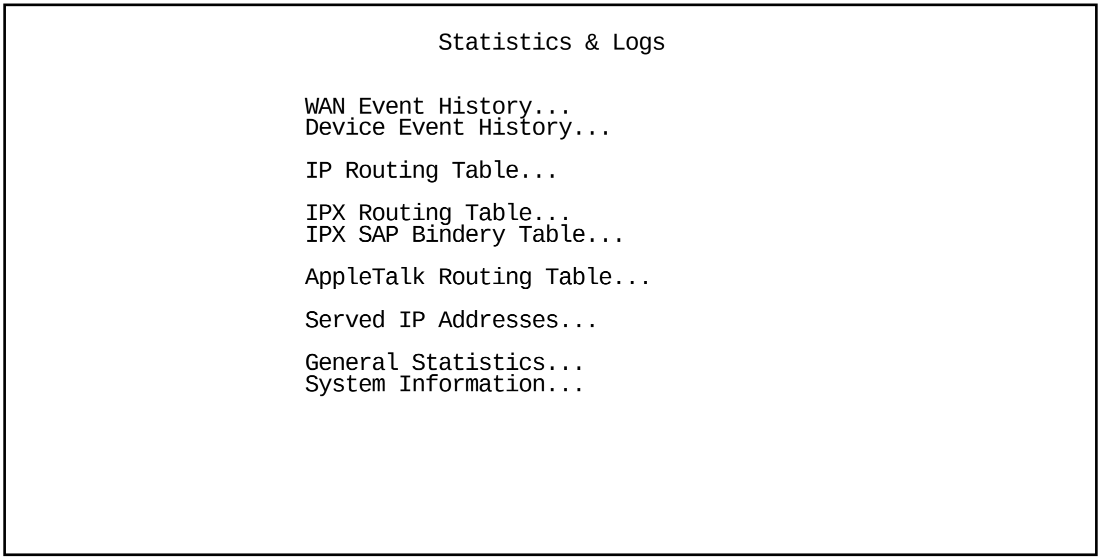
- The number of bytes and packets received through the channel
- The number of bytes and packets transmitted through the channel

Event Histories

The Netopia R2020 records certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the router's system and one for the WAN. The Netopia R2020's built-in battery backup prevents loss of event history from a shut down or reset.

The Router's event histories are structured to display the most recent events first, and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk. Both the WAN Event History and the Device Event History retain records of the 128 most recent events.

To go to the Event Histories screens, select either **WAN Event History** or **Device Event History** in the Statistics & Logs screen.

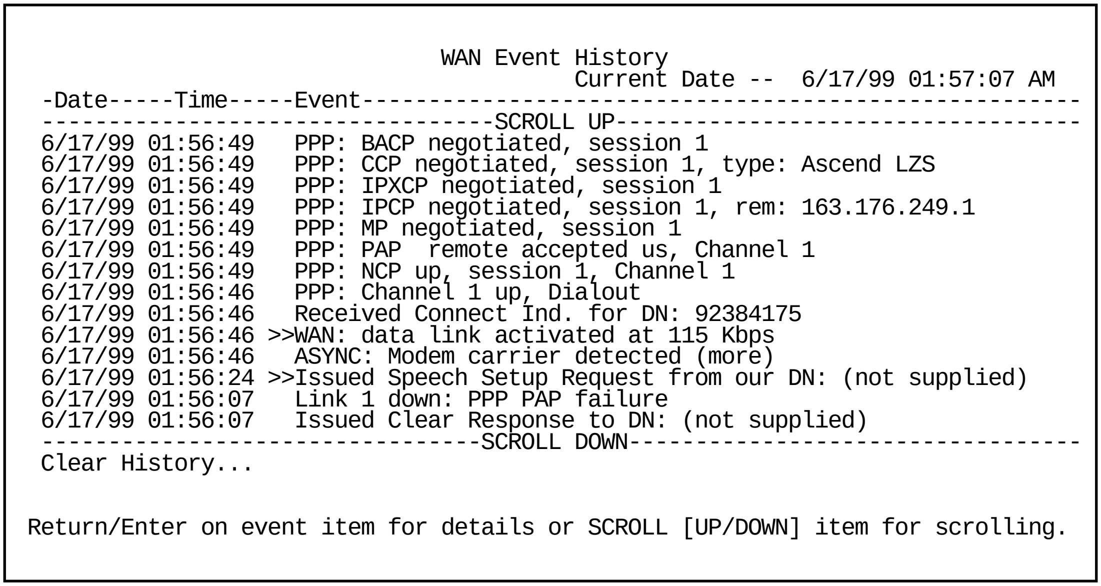


```
                         Statistics & Logs


                    WAN Event History...
                    Device Event History...

                    IP Routing Table...

                    IPX Routing Table...
                    IPX SAP Bindery Table...

                    AppleTalk Routing Table...

                    Served IP Addresses...

                    General Statistics...
                    System Information...
```

WAN Event History

The WAN Event History screen lists a total of 128 events on the WAN. The most recent events appear at the top.

To go to the WAN Event History screen, select **WAN Event History** in the Statistics & Logs screen.



```
                               WAN Event History
                                         Current Date --  6/17/99 01:57:07 AM
 -Date-----Time-----Event------------------------------------------------------
 ----------------------------------SCROLL UP-----------------------------------
 6/17/99 01:56:49   PPP: BACP negotiated, session 1
 6/17/99 01:56:49   PPP: CCP negotiated, session 1, type: Ascend LZS
 6/17/99 01:56:49   PPP: IPXCP negotiated, session 1
 6/17/99 01:56:49   PPP: IPCP negotiated, session 1, rem: 163.176.249.1
 6/17/99 01:56:49   PPP: MP negotiated, session 1
 6/17/99 01:56:49   PPP: PAP  remote accepted us, Channel 1
 6/17/99 01:56:49   PPP: NCP up, session 1, Channel 1
 6/17/99 01:56:46   PPP: Channel 1 up, Dialout
 6/17/99 01:56:46   Received Connect Ind. for DN: 92384175
 6/17/99 01:56:46 >>WAN: data link activated at 115 Kbps
 6/17/99 01:56:46   ASYNC: Modem carrier detected (more)
 6/17/99 01:56:24 >>Issued Speech Setup Request from our DN: (not supplied)
 6/17/99 01:56:07   Link 1 down: PPP PAP failure
 6/17/99 01:56:07   Issued Clear Response to DN: (not supplied)
 ---------------------------------SCROLL DOWN----------------------------------
 Clear History...


Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.
```

Each entry in the list contains the following information:

Time: Time of the event.

Date: Date of the event.

Event: A brief description of the event.

Ch.: The channel involved in the event.

Dir. Number: The directory number (number dialed) involved in the event.

The first event in each call sequence is marked with double arrows (>>).

Failures are marked with an asterisk (*).

If the event history exceeds the size of the screen, you can scroll through it by using the **SCROLL UP** and **SCROLL DOWN** items.

To scroll up, select the **SCROLL UP** item at the top of the list and press the Return key. To scroll down, select the **SCROLL DOWN** item at the bottom of the list and press the Return key.

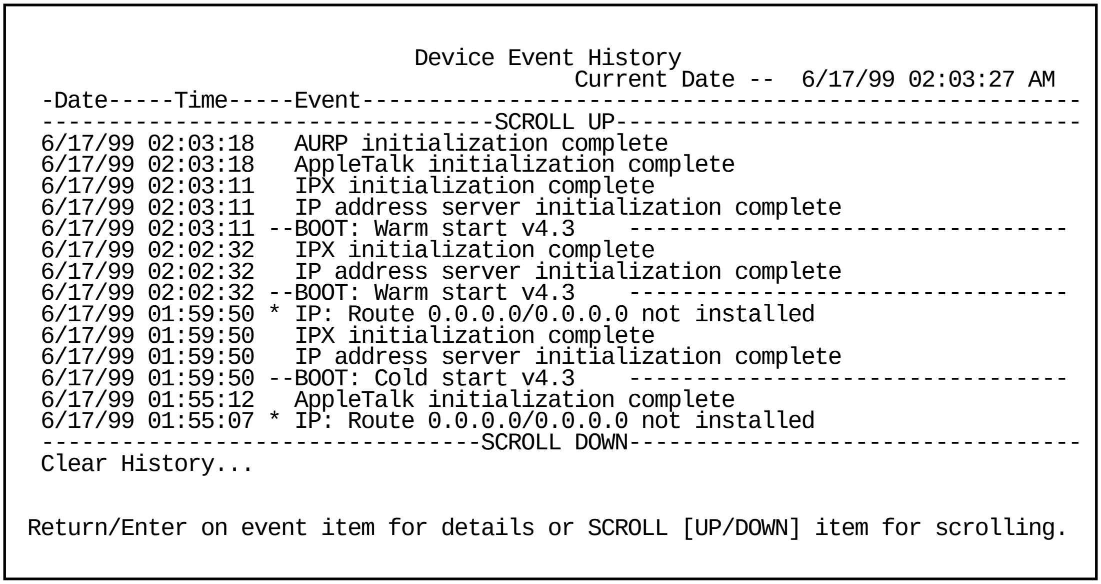
To get more information about any event listed in the WAN Event History, select the event and then press the Return key. A dialog box containing more information about the selected event will appear. Press Return or the Escape key to dismiss the dialog box.

To clear the Event History, select **Clear History** at the bottom of the history screen and press Return.

Device Event History

The Device Event History screen lists a total of 128 port and system events, giving the time and date for each event, as well as a brief description. The most recent events appear at the top.

To go to the Device Event History screen, select **Device Event History** in the Statistics & Logs screen.



```
                              Device Event History
                                          Current Date --  6/17/99 02:03:27 AM
 -Date-----Time-----Event-------------------------------------------------------
 ---------------------------------SCROLL UP-------------------------------------
 6/17/99 02:03:18   AURP initialization complete
 6/17/99 02:03:18   AppleTalk initialization complete
 6/17/99 02:03:11   IPX initialization complete
 6/17/99 02:03:11   IP address server initialization complete
 6/17/99 02:03:11 --BOOT: Warm start v4.3    ---------------------------------
 6/17/99 02:02:32   IPX initialization complete
 6/17/99 02:02:32   IP address server initialization complete
 6/17/99 02:02:32 --BOOT: Warm start v4.3    ---------------------------------
 6/17/99 01:59:50 * IP: Route 0.0.0.0/0.0.0.0 not installed
 6/17/99 01:59:50   IPX initialization complete
 6/17/99 01:59:50   IP address server initialization complete
 6/17/99 01:59:50 --BOOT: Cold start v4.3    ---------------------------------
 6/17/99 01:55:12   AppleTalk initialization complete
 6/17/99 01:55:07 * IP: Route 0.0.0.0/0.0.0.0 not installed
 --------------------------------SCROLL DOWN------------------------------------
 Clear History...


Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.
```

If the event history exceeds the size of the screen, you can scroll through it by using the **SCROLL UP** and **SCROLL DOWN** items.

To scroll up, select the **SCROLL UP** item at the top of the list and press the Return key. To scroll down, select the **SCROLL DOWN** item at the bottom of the list and press Return.

To obtain more information about any event listed in the Device Event History, select the event and then press Return. A dialog box containing more information about the selected event will appear. Press Return or the Escape key to dismiss the dialog box.

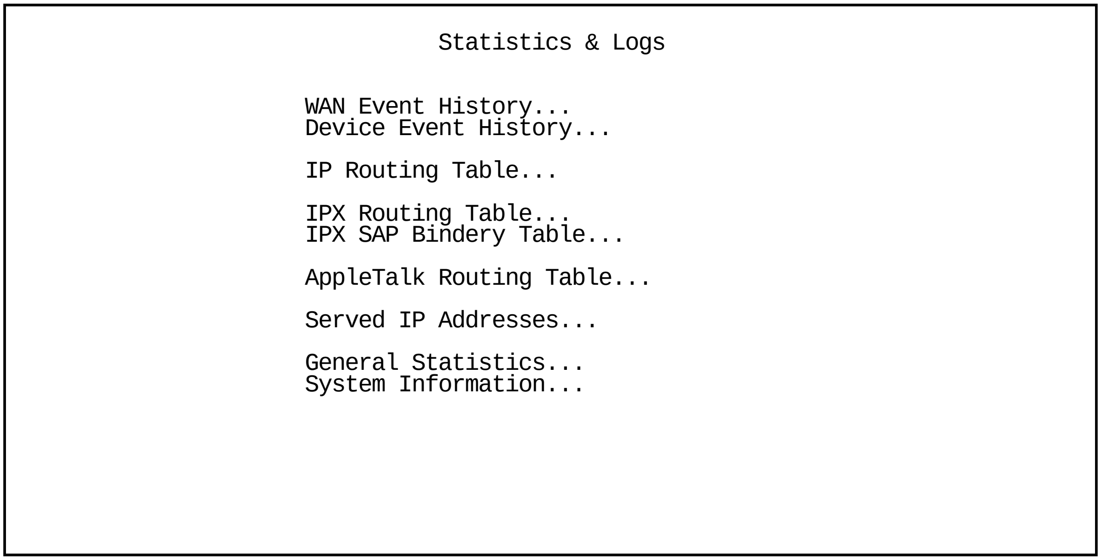
To clear the Device Event History, select **Clear Device Event History** in the Event Histories screen and press Return.

Routing Tables

You can view all of the IP, IPX and AppleTalk routes in the Netopia R2020’s IP, IPX and AppleTalk routing tables, respectively.

To go to a Routing Table screen, select the Routing Table you are interested in from the **Statistics & Logs** screen.

Each of the routing table screens represents a “snapshot” of the routing table information at the time the screen is first invoked. To take a new snapshot, select **Update** at the bottom of the screen and press Return.

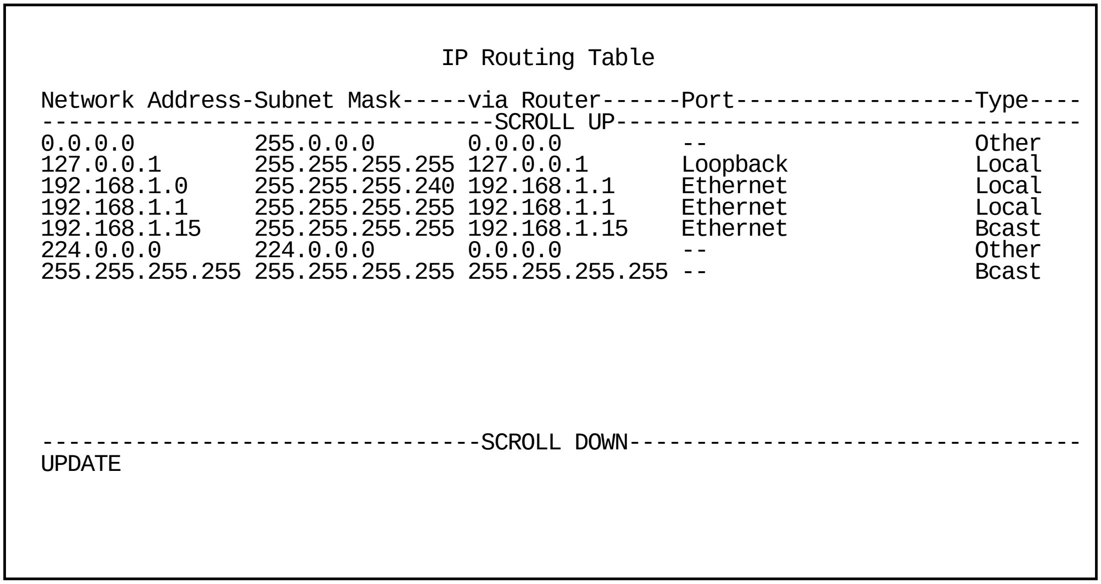


```
                         Statistics & Logs

               WAN Event History...
               Device Event History...

               IP Routing Table...

               IPX Routing Table...
               IPX SAP Bindery Table...

               AppleTalk Routing Table...

               Served IP Addresses...

               General Statistics...
               System Information...
```

IP routing table

The IP routing table displays all of the IP routes currently known to the Netopia R2020.

To display the IP Routing Table screen, select **IP Routing Table** in the Statistics & Logs screen and press Return.



```
                              IP Routing Table

Network Address-Subnet Mask-----via Router------Port------------------Type----
----------------------------------SCROLL UP-----------------------------------
0.0.0.0         255.0.0.0       0.0.0.0         --                    Other
127.0.0.1       255.255.255.255 127.0.0.1       Loopback              Local
192.168.1.0     255.255.255.240 192.168.1.1     Ethernet              Local
192.168.1.1     255.255.255.255 192.168.1.1     Ethernet              Local
192.168.1.15    255.255.255.255 192.168.1.15    Ethernet              Bcast
224.0.0.0       224.0.0.0       0.0.0.0         --                    Other
255.255.255.255 255.255.255.255 255.255.255.255 --                    Bcast






---------------------------------SCROLL DOWN----------------------------------
UPDATE
```

IPX routing table

The IPX routing table displays all of the IPC routes currently known to the Netopia R2020.

To display the IPX Routing Table screen, select **IPX Routing Table** in the Statistics & Logs screen and press Return.

IPX Sap Bindery table

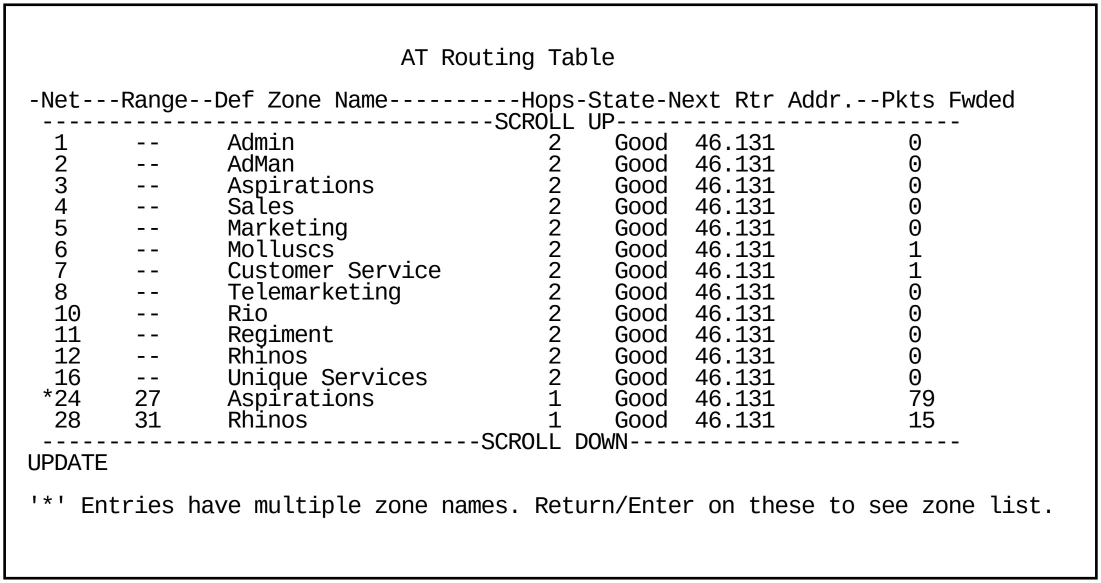
The IPX Sap Bindery table displays all of the IPX Sap Bindery routes currently known to the Netopia R2020.

To display the IPX SAP Bindery Table screen, select **IPX Sap Bindery Table** in the Statistics & Logs screen and press Return.

AppleTalk routing table

The AppleTalk routing table displays information about the current state of AppleTalk networks connected to the Netopia R2020, including remote AppleTalk networks connected with AURP. This information is gathered from other active AppleTalk routers.

To display the AppleTalk Routing Table screen, select **AppleTalk Routing Table** in the Statistics & Logs screen and press Return.



```
                            AT Routing Table

-Net---Range--Def Zone Name----------Hops-State-Next Rtr Addr.--Pkts Fwded
 ----------------------------------SCROLL UP-------------------------
  1     --     Admin                   2    Good  46.131          0
  2     --     AdMan                   2    Good  46.131          0
  3     --     Aspirations             2    Good  46.131          0
  4     --     Sales                   2    Good  46.131          0
  5     --     Marketing               2    Good  46.131          0
  6     --     Molluscs                2    Good  46.131          1
  7     --     Customer Service        2    Good  46.131          1
  8     --     Telemarketing           2    Good  46.131          0
  10    --     Rio                     2    Good  46.131          0
  11    --     Regiment                2    Good  46.131          0
  12    --     Rhinos                  2    Good  46.131          0
  16    --     Unique Services         2    Good  46.131          0
 *24    27     Aspirations             1    Good  46.131          79
  28    31     Rhinos                  1    Good  46.131          15
 ---------------------------------SCROLL DOWN------------------------
UPDATE

'*' Entries have multiple zone names. Return/Enter on these to see zone list.
```

Each row in the AppleTalk routing table corresponds to an AppleTalk route or network range. If the list of routes shown exceeds the size of the screen, you can scroll through it by using the **SCROLL UP** and **SCROLL DOWN** items.

To scroll up, select the **SCROLL UP** item at the top of the table and press the Return key. To scroll down, select the **SCROLL DOWN** item at the bottom of the table and press the Return key.

The table has the following columns:

Net: Displays the starting network number supplied by the AppleTalk router in the ‘Next Rtr Addr. Column’. If a network number is preceded by an asterisk (*), it has multiple zones. To display the zones, select the network entry and press Return.

Range: Displays the ending network number for the extended network.

(Def) Zone Name: Displays the zone or zones associated with the specified network or network range. The zone name shown is either the only zone or the default zone name for an extended network. To see the complete list of zones for an extended network with multiple zones, select the entry in the table and press the Return key. Press the Return key again to close the list of zones.

Hops: Displays the number of routers between the Netopia R2020 and the specified network.

State: Displays the state of the specified route, based on the frequency of Routing Table Maintenance Protocol (RTMP) packets received for the route. The state can be Good, Suspect, or Bad. AppleTalk routers regularly exchange RTMP packets to update AppleTalk routing information.

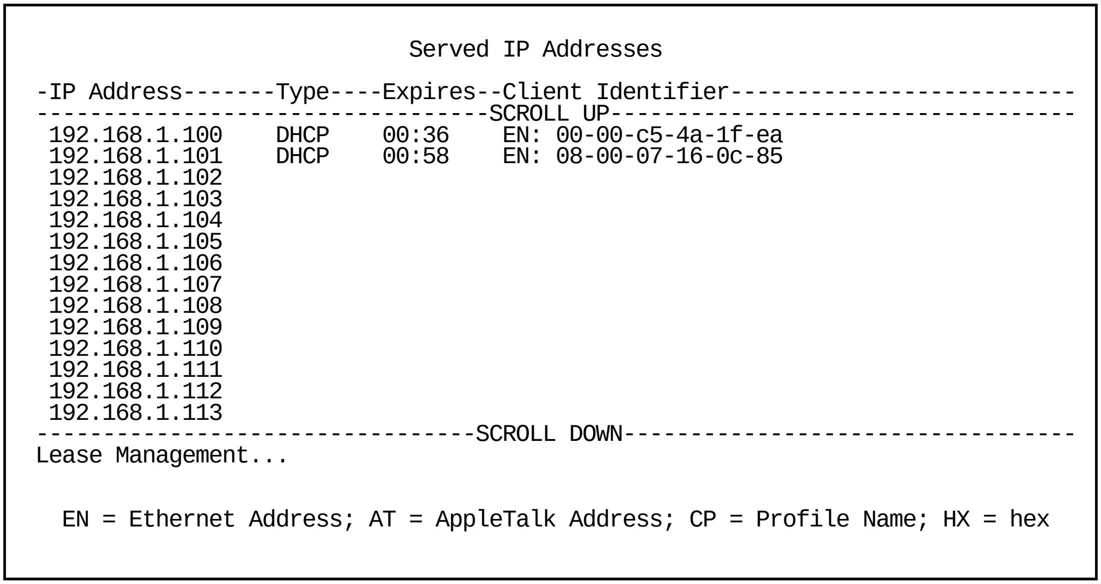
Next Rtr Addr.: Displays the DDP or IP address of the next hop for the specified route. A DDP address is displayed if the router shown is on the local AppleTalk network. DDP address means that a connection to the next hop router is by a native AppleTalk network (e.g.: LocalTalk or EtherTalk Phase II). An IP address is displayed if the Netopia R2020 is connected to the router shown using AURP. IP address means a connection transports over AURP (AppleTalk encapsulated IP).

Pkts Fwded: The number of packets sent to the router shown.

Served IP Addresses

You can view all of the IP addresses currently being served by the Netopia R2020 Dual Analog Router from the **Served IP Addresses** screen. From the Statistics & Logs menu, select Served IP Addresses.

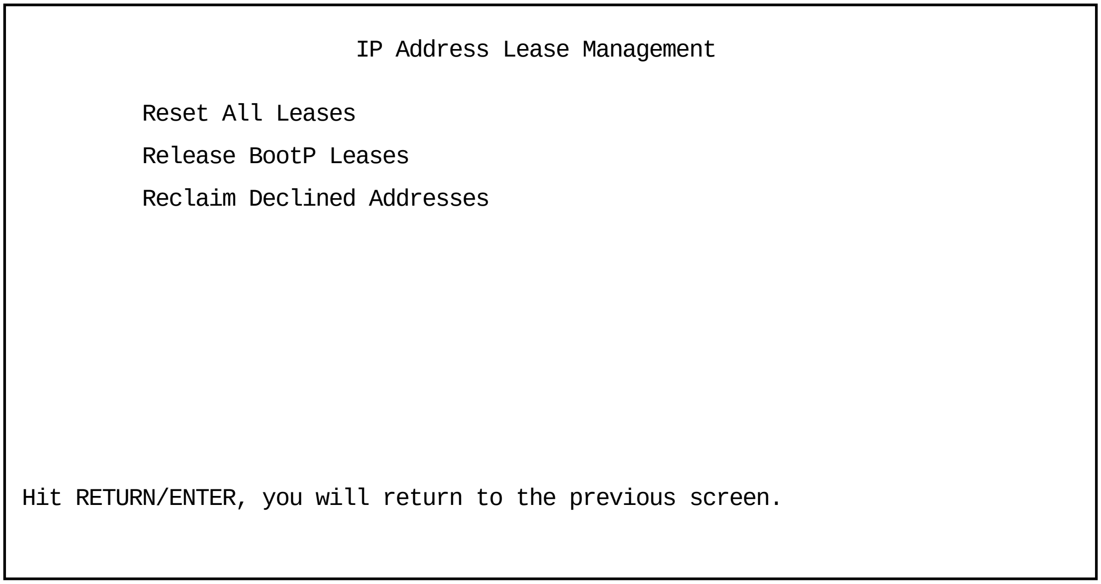
The Served IP Addresses screen appears.



```
                           Served IP Addresses

-IP Address-------Type----Expires--Client Identifier--------------------------
----------------------------------SCROLL UP-----------------------------------
 192.168.1.100    DHCP    00:36    EN: 00-00-c5-4a-1f-ea
 192.168.1.101    DHCP    00:58    EN: 08-00-07-16-0c-85
 192.168.1.102
 192.168.1.103
 192.168.1.104
 192.168.1.105
 192.168.1.106
 192.168.1.107
 192.168.1.108
 192.168.1.109
 192.168.1.110
 192.168.1.111
 192.168.1.112
 192.168.1.113
---------------------------------SCROLL DOWN----------------------------------
Lease Management...


  EN = Ethernet Address; AT = AppleTalk Address; CP = Profile Name; HX = hex
```

You can manage DHCP leases by selecting **Lease Management** in this screen.

The IP Address Lease Management screen appears.



```
                          IP Address Lease Management

                Reset All Leases

                Release BootP Leases

                Reclaim Declined Addresses










Hit RETURN/ENTER, you will return to the previous screen.
```

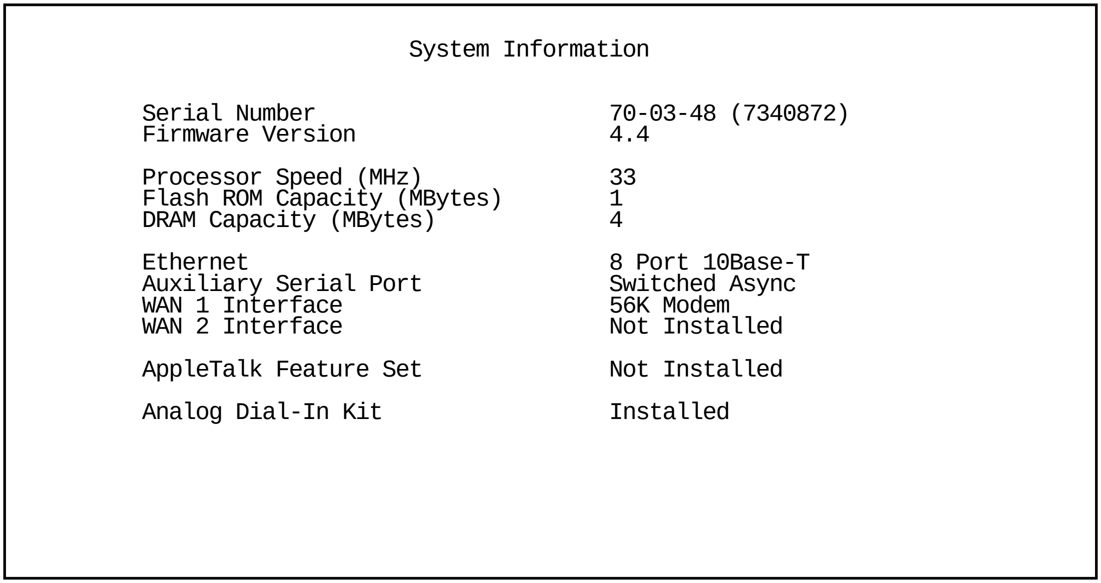
By selecting each of these options you can:

- **Reset** all current IP addresses leased through DHCP without waiting for the default one hour lease period to elapse
- **Release** BootP leases that may be in place, and which may no longer be required
- **Reclaim** served leases that have been declined, for example by devices which may no longer be on the network.

System Information

The System Information screen gives a summary view of the general system level values in the Netopia R2020 Dual Analog Router. From the Statistics & Logs menu select **System Information**.

The System Information screen appears.



```
                       System Information

          Serial Number                     70-03-48 (7340872)
          Firmware Version                  4.4

          Processor Speed (MHz)             33
          Flash ROM Capacity (MBytes)       1
          DRAM Capacity (MBytes)            4

          Ethernet                          8 Port 10Base-T
          Auxiliary Serial Port             Switched Async
          WAN 1 Interface                   56K Modem
          WAN 2 Interface                   Not Installed

          AppleTalk Feature Set             Not Installed

          Analog Dial-In Kit                Installed
```

SNMP

The Netopia R2020 includes a Simple Network Management Protocol (SNMP) agent, allowing monitoring and configuration by a standard SNMP manager.

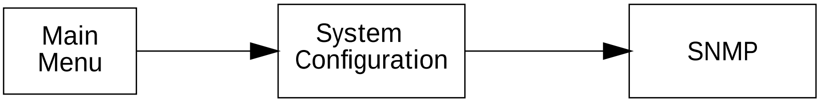
The Netopia R2020 supports the following Management Information Base (MIB) documents:

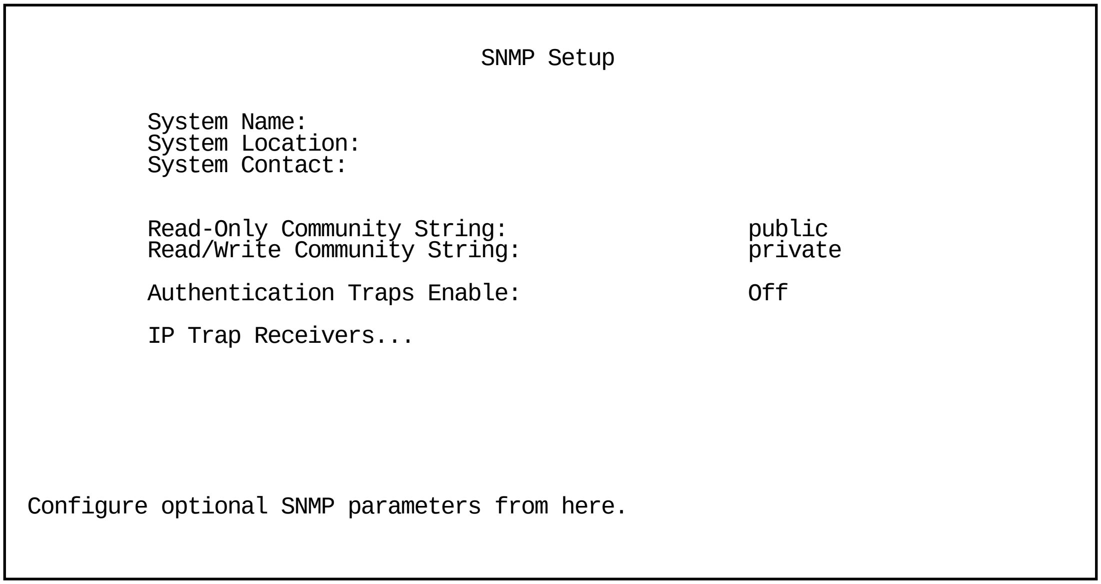
- MIB II (RFC 1213)
- Interface MIB (RFC 1229)
- Ethernet MIB (RFC 1643)
- AppleTalk MIB-I (RFC 1243)
- Frame Relay DTE MIB (RFC 1315)
- Netopia MIB

These MIBs are on the Netopia R2020 CD included with the Netopia R2020. You should load these MIBs into your SNMP management software in the order they are listed here. Follow the instructions included with your SNMP manager on how to load MIBs.

The SNMP Setup screen

To go to the SNMP Setup screen from the Main Menu, select **SNMP** in the System Configuration screen and press Return.





```
                              SNMP Setup


          System Name:
          System Location:
          System Contact:


          Read-Only Community String:                   public
          Read/Write Community String:                  private

          Authentication Traps Enable:                  Off

          IP Trap Receivers...





 Configure optional SNMP parameters from here.
```

Follow these steps to configure the first three items in the screen:

1. Select **System Name** and enter a descriptive name for the Netopia R2020's SNMP agent.
2. Select **System Location** and enter the router's physical location (room, floor, building, etc.).
3. Select **System Contact** and enter the name of the person responsible for maintaining the router.

System Name, **System Location**, and **System Contact** set the values returned by the Netopia R2020 SNMP agent for the SysName, SysLocation, and SysContact objects, respectively, in the MIB-II system group. Although optional, the information you enter in these items can help a system administrator manage the network more efficiently.

Community strings

The **Read-Only Community String** and the **Read / Write Community String** are like passwords that must be used by an SNMP manager querying or configuring the Netopia R2020. An SNMP manager using the **Read-Only Community String** can examine statistics and configuration information from the router, but cannot modify the router's configuration. An SNMP manager using the **Read / Write Community String** can both examine and modify configuration parameters.

By default, the read-only and read/write community strings are set to "public" and "private," respectively. You should change both of the default community strings to values known only to you and trusted system administrators.

To change a community string, select it and enter a new value.

Starting with the version 4.3 firmware, setting the Read-Only and Read-Write community strings to the empty string will block all SNMP requests to the router. (The router may still send SNMP Traps if those are properly enabled.)

Previously, if either community string was the empty string, SNMP Requests specifying an empty community string were accepted and processed.

This change is designed to allow the administrator to block SNMP access to the router, and to provide more granular control over the allowed SNMP operations to the router.

- Setting only the Read-Write community string to the empty string will block SNMP Set Requests to the router, but Get Requests and Get-Next Requests will still be honored using the Read-Only community string (assuming that is not the empty string).
- Setting only the Read-Only community string to the empty string will *not* block Get Requests or Get-Next Requests since those operations (and Set Requests) are still allowed using the (non-empty) Read-Write community string.

Caution!

Even if you decide not to use SNMP, you should change the community strings. This prevents unauthorized access to the Netopia R2020 through SNMP. For more information on security issues, see "Suggested security measures" on page 14-1.

SNMP traps

An SNMP **trap** is an informational message sent from an SNMP agent (in this case, the Netopia R2020) to a manager. When a manager receives a trap, it may log the trap as well as generate an alert message of its own.

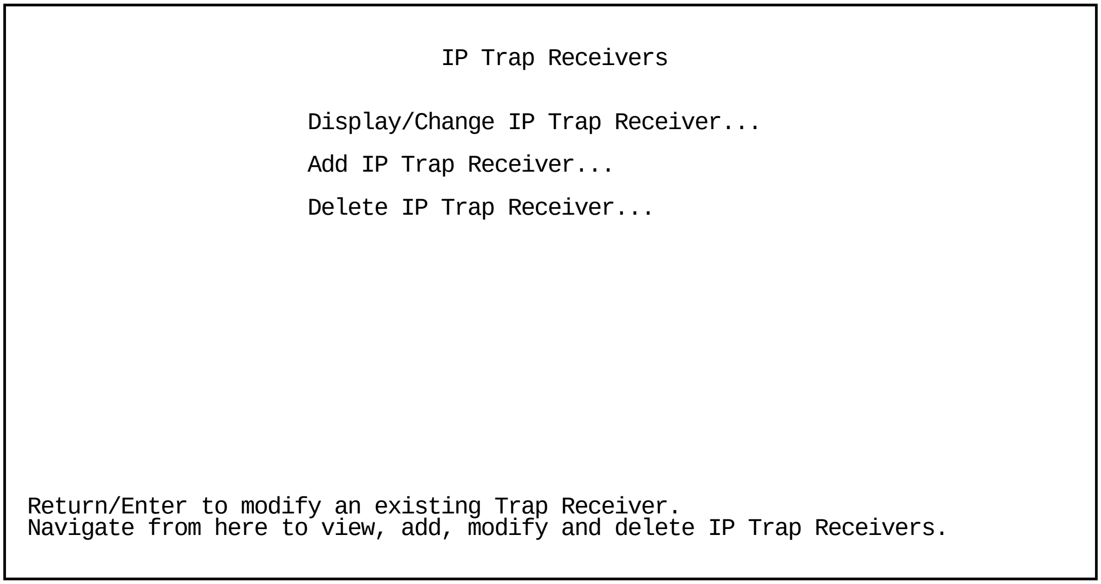
Standard traps generated by the Netopia R2020 include the following:

- An authentication failure trap is generated when the router detects an incorrect community string in a received SNMP packet. **Authentication Traps Enable** must be **On** for this trap to be generated.
- A cold start trap is generated after the router is reset.
- An interface down trap (ifDown) is generated when one of the router's interfaces, such as a port, stops functioning or is disabled.
- An interface up trap (ifUp) is generated when one of the router's interfaces, such as a port, begins functioning.

The Netopia R2020 sends traps using UDP (for IP networks).

You can specify which SNMP managers are sent the IP traps generated by the Netopia R2020. Up to eight receivers can be set. You can also review and remove IP traps.

Go to the IP Trap Receivers screen by selecting **IP Trap Receivers** in the SNMP Setup screen.



```
                              IP Trap Receivers

                    Display/Change IP Trap Receiver...

                    Add IP Trap Receiver...

                    Delete IP Trap Receiver...










Return/Enter to modify an existing Trap Receiver.
Navigate from here to view, add, modify and delete IP Trap Receivers.
```

Setting the IP trap receivers

1. Select **Add IP Trap Receiver**.
2. Select **Receiver IP Address or Domain Name**. Enter the IP address or domain name of the SNMP manager you want to receive the trap.
3. Select **Community String** if you enabled one in the SNMP Setup screen, and enter the appropriate password.
4. Select **Add Trap Receiver Now** and press Return. You can add up to seven more receivers.

Viewing IP trap receivers

To display a view-only table of IP trap receivers, select **Display / Change IP Trap Receiver** in the IP Trap Receivers screen.

Modifying IP trap receivers

1. To edit an IP trap receiver, select **Display / Change IP Trap Receiver** in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the Change IP Trap Receiver screen, edit the information as needed and press Return.

Deleting IP trap receivers

1. To delete an IP trap receiver, select **Delete IP Trap Receiver** in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the dialog box, select **Continue** and press Return.

Chapter 14

Security

The Netopia R2020 provides a number of security features to help protect its configuration screens and your local network from unauthorized access. Although these features are optional, it is strongly recommended that you use them.

This section covers the following topics:

- "Suggested security measures" on page 14-1, lists actions for blocking potential security holes.
- "User accounts," beginning on page 14-2, shows you how to set up name/password combinations to protect the Netopia R2020's configuration screens.
- "Dial-in Console Access" on page 14-3
- "Telnet access" on page 14-4, shows you how to control access to the Netopia R2020 by those using the Telnet protocol.
- "About filters and filter sets," beginning on page 14-4, and "Working with IP filters and filter sets," beginning on page 14-12, have information on what filters are, how they work, how to customize them, and how to use them in sets. For information on IPX filters and filter sets, see "IPX filters," beginning on page 14-21.
- "Firewall tutorial" on page 14-28
- "Token Security Authentication" on page 14-36

Suggested security measures

In addition to setting up user accounts, Telnet access, and filters (all of which are covered later in this chapter), there are other actions you can take to make the Netopia R2020 and your network more secure:

- Change the SNMP community strings (or passwords). The default community strings are universal and could easily be known to a potential intruder.
- Set the answer profile so it must match incoming calls to a connection profile.
- Use CallerID.
- Leave the "Enable Dial-in Console Access" option set to No.
- Where possible, insist on using PAP, CHAP, or secure authentication token card to authenticate connections to and from connection profiles.
- When using AURP, accept connections only from configured partners.
- Configure the Netopia R2020 through the serial console port to ensure that your communications cannot be intercepted.

User accounts

When you first set up and configure the Netopia R2020, no passwords are required to access the configuration screens. Anyone could tamper with the router's configuration by simply connecting it to a console.

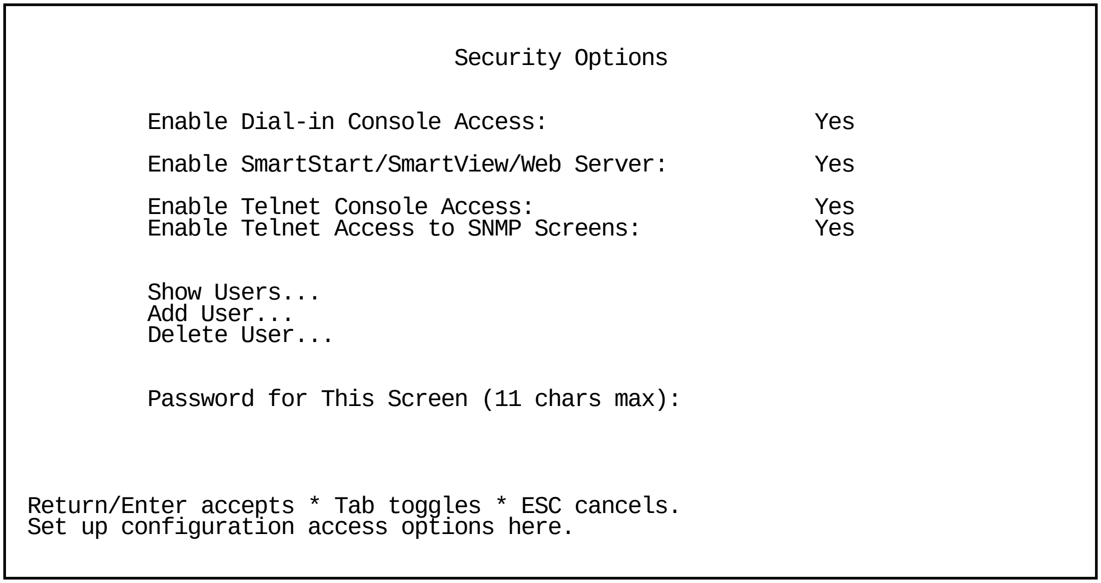
However, by adding user accounts, you can protect the most sensitive screens from unauthorized access. User accounts are composed of name/password combinations that can be given to authorized users.

Caution!

You are strongly encouraged to add protection to the configuration screens. Unprotected screens could allow an unauthorized user to compromise the operation of your entire network.

Once user accounts are created, users who attempt to access protected screens will be challenged. Users who enter an incorrect name or password are returned to a screen requesting a name/password combination to access the Main Menu.

To set up user accounts, select **Security** in the System Configuration screen and go to the Security Options screen.



```
                          Security Options

         Enable Dial-in Console Access:                   Yes

         Enable SmartStart/SmartView/Web Server:          Yes

         Enable Telnet Console Access:                    Yes
         Enable Telnet Access to SNMP Screens:            Yes


         Show Users...
         Add User...
         Delete User...


         Password for This Screen (11 chars max):



Return/Enter accepts * Tab toggles * ESC cancels.
Set up configuration access options here.
```

Protecting the Security Options screen

The first screen you should protect is the Security Options screen, because it controls access to the configuration screens. Access to the Security Options screen can be protected with a password.

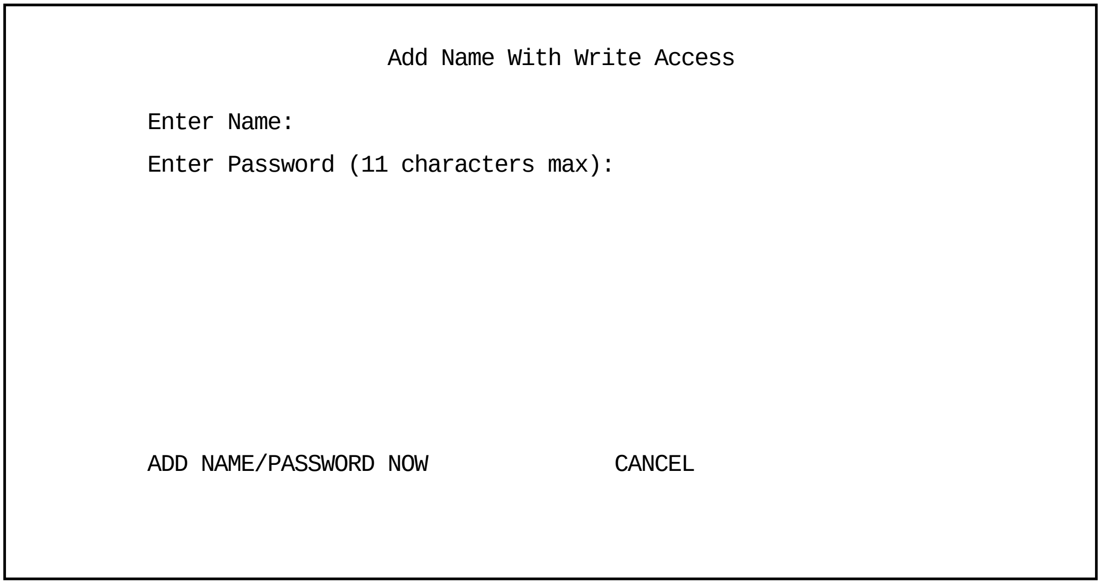
Select **Password for This Screen** in the Security Options screen and enter a password. Make sure this password is secure and is different from any of the user account passwords.

Protecting the configuration screens

You can protect the configuration screens with user accounts. You can administer the accounts from the Security Options screen. You can create up to four accounts.

To display a view-only list of user accounts, select **Show Users** in the Security Options screen.

To add a new user account, select **Add User** in the Security Options screen and press Return to go to the Add Name With Write Access screen.



```
                    Add Name With Write Access

         Enter Name:

         Enter Password (11 characters max):








         ADD NAME/PASSWORD NOW              CANCEL
```

Follow these steps to configure the new account:

1. Select **Enter Name** and enter a descriptive name (for example, the user’s first name).
2. Select **Enter Password** and enter a password.
3. To accept the new name/password combination, select **ADD NAME/PASSWORD NOW**. To exit the Add Name With Write Access screen without saving the new account, select **CANCEL**.

To delete a user account, select **Delete User** to display a list of accounts. Select an account from the list and press Return to delete it. To exit the list without deleting the selected account, press the Escape key.

Dial-in Console Access

Remote modem terminal emulator setups can dial in to either internal modem line and establish a remote console session, even though they are not using PPP. This allows Netopia Inc.'s “Up and Running, Guaranteed!” department or other administrator with the appropriate security to remotely configure your router for you. If you used SmartStart to configure your router, this option will be set to “No”.

- To prevent any remote caller from establishing a remote session, leave the option **Enable Dial-in Console Access** set to “No”.
- To allow access for Up and Running, Guaranteed! with the default name and password in place, toggle this option to “Yes”.

Enable SmartStart/Web Server

You may wish to restrict access to the web-based screens to prevent inadvertent switching or connecting and disconnecting of Connection Profiles. Since SmartStart can be used to reconfigure the router, you may wish to block inadvertent damage resulting from unauthorized use of SmartStart. To prevent access to these features toggle this option to “No”.

Telnet access

Telnet is a TCP/IP service that allows remote terminals to access hosts on an IP network. The Netopia R2020 supports Telnet access to its configuration screens.

Caution!

You should consider password-protecting or restricting Telnet access to the Netopia R2020 if you suspect there is a chance of tampering.

To password-protect the configuration screens, select Easy Setup from the Main Menu, and go to the **Easy Setup Security Configuration** screen. By entering a Name and Password pair in this screen, all access via serial, Telnet, SNMP, and web server will be password-protected.

To restrict Telnet access, select **Security** in the Advanced Configuration Menu and go to the Security Options screen. There are two levels of Telnet restriction available:

To restrict Telnet access to the SNMP screens, select **Enable Telnet Access to SNMP Screens** and toggle it to **No**. (See “SNMP traps” on page 13-14.)

To restrict Telnet access to all of the configuration screens, select **Enable Telnet Console Access** and toggle it to **No**.

About filters and filter sets

Security should be a high priority for anyone administering a network connected to the Internet. Using packet filters to control network communications can greatly improve your network's security.

The Netopia R2020's packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the router's filter sets for a variety of packet filtering applications. Typically, you use filters to selectively admit or refuse TCP/IP connections from certain remote networks and specific hosts. You will also use filters to screen particular types of connections. This is commonly called firewalling your network.

Before creating filter sets, you should read the next few sections to learn more about how these powerful security tools work.

What's a filter and what's a filter set?

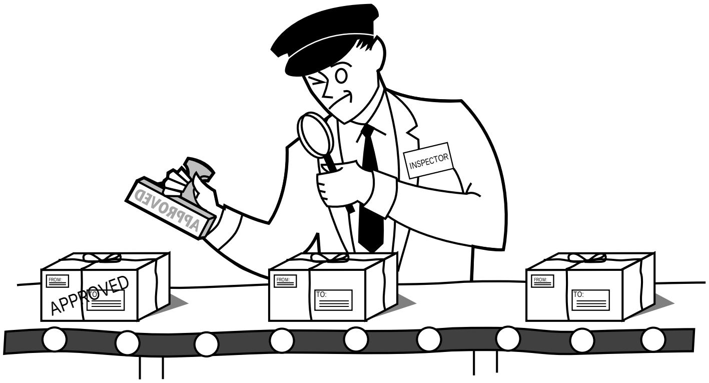
A filter is a rule that lets you specify what sort of data can flow in and out of your network. A particular filter can either be an input filter—one that is used on data (packets) coming in to your network from the Internet—or an output filter—one that is used on data (packets) going out from your network to the Internet.

A filter set is a group of filters that work together to check incoming or outgoing data. A filter set can consist of a combination of input and output filters.

How filter sets work

A filter set acts like a team of customs inspectors. Each filter is an inspector through which incoming and outgoing packages must pass. The inspectors work as a team, but each inspects every package individually.

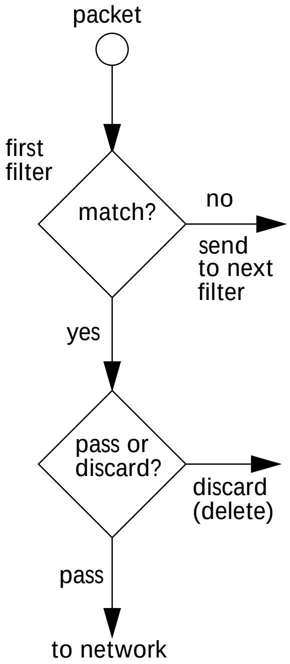
Each inspector has a specific task. One inspector's task may be to examine the destination address of all outgoing packages. That inspector looks for a certain destination—which could be as specific as a street address or as broad as an entire country—and checks each package's destination address to see if it matches that destination.



A filter inspects data packets like a customs inspector scrutinizing packages.

Filter priority

Continuing the customs inspectors analogy, imagine the inspectors lined up to examine a package. If the package matches the first inspector's criteria, the package is either rejected or passed on to its destination, depending on the first inspector's particular orders. In this case, the package is never seen by the remaining inspectors.



If the package does not match the first inspector's criteria, it goes to the second inspector, and so on. You can see that the order of the inspectors in the line is very important.

For example, let's say the first inspector's orders are to send along all packages that come from Rome, and the second inspector's orders are to reject all packages that come from France. If a package arrives from Rome, the first inspector sends it along without allowing the second inspector to see it. A package from Paris is ignored by the first inspector, rejected by the second inspector, and never seen by the others. A package from London is ignored by the first two inspectors, and so it's seen by the third inspector.

In the same way, filter sets apply their filters in a particular order. The first filter applied can pass or discard a packet before that packet ever reaches any of the other filters. If the first filter can neither pass nor discard the packet (because it cannot match any criteria), the second filter has a chance to pass or reject it, and so on. Because of this hierarchical structure, each filter is said to have a priority. The first filter has the highest priority, and the last filter has the lowest priority.

How individual filters work

As described above, a filter applies criteria to an IP packet and then takes one of three actions:

A filter's actions

- Passes the packet to the local or remote network
- Blocks (discards) the packet
- Ignores the packet

A filter passes or blocks a packet only if it finds a match after applying its criteria. When no match occurs, the filter ignores the packet.

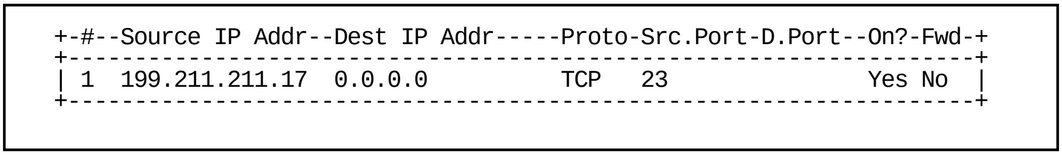
The criteria are based on information contained in the packets. A filter is simply a rule that prescribes certain actions based on certain conditions. For example, the following rule qualifies as a filter:

A filtering rule

Block all Telnet attempts that originate from the remote host 199.211.211.17.

This rule applies to Telnet packets that come from a host with the IP address 199.211.211.17. If a match occurs, the packet is blocked.

Here is what this rule looks like when implemented as a filter on the Netopia R2020:



```
+-#--Source IP Addr--Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+--------------------------------------------------------------------+
| 1  199.211.211.17  0.0.0.0          TCP   23               Yes No  |
+--------------------------------------------------------------------+
```

To understand this particular filter, look at the parts of a filter.

Parts of a filter

A filter consists of criteria based on packet attributes. A typical filter can match a packet on any one of the following attributes:

- The source IP address (where the packet was sent from)
- The destination IP address (where the packet is going)
- The type of higher-layer Internet protocol the packet is carrying, such as TCP or UDP

Port numbers

A filter can also match a packet's port number attributes, but only if the filter's protocol type is set to TCP or UDP, since only those protocols use port numbers. The filter can be configured to match the following:

- The source port number (the port on the sending host that originated the packet)
- The destination port number (the port on the receiving host that the packet is destined for)

By matching on a port number, a filter can be applied to selected TCP or UDP services, such as Telnet, FTP, and World Wide Web. The tables below show a few common services and their associated port numbers.

Internet service	TCP port	Internet service	TCP port
FTP	20/21	Finger	79
Telnet	23	World Wide Web	80
SMTP (mail)	25	News	144
Gopher	70	rlogin	513
Internet service	**UDP port**	**Internet service**	**UDP port**
Who Is	43	AppleTalk Routing Maintenance (at-rtmp)	202
World Wide Web	80	AppleTalk Name Binding (at-nbp)	202
SNMP	161	AURP (AppleTalk)	387
TFTP	69	who	513

Port number comparisons

A filter can also use a comparison option to evaluate a packet's source or destination port number. The comparison options are:

No Compare: No comparison of the port number specified in the filter with the packet's port number.

Not Equal To: For the filter to match, the packet's port number cannot equal the port number specified in the filter.

Less Than: For the filter to match, the packet's port number must be less than the port number specified in the filter.

Less Than or Equal: For the filter to match, the packet's port number must be less than or equal to the port number specified in the filter.

Equal: For the filter to match, the packet's port number must equal the port number specified in the filter.

Greater Than: For the filter to match, the packet's port number must be greater than the port number specified in the filter.

Greater Than or Equal: For the filter to match, the packet's port number must be greater than or equal to the port number specified in the filter.

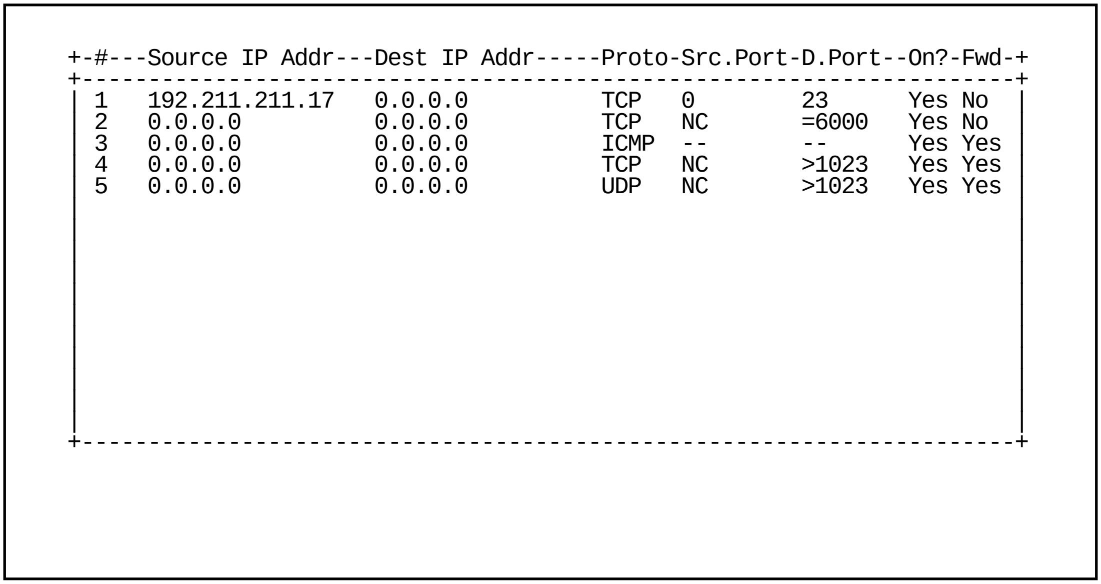
Other filter attributes

There are three other attributes to each filter:

- The filter's order (i.e., priority) in the filter set
- Whether the filter is currently active
- Whether the filter is set to pass (forward) packets or to block (discard) packets

Putting the parts together

When you display a filter set, its filters are displayed as rows in a table:



```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+----------------------------------------------------------------------+
| 1   192.211.211.17   0.0.0.0          TCP   0        23      Yes No  |
| 2   0.0.0.0          0.0.0.0          TCP   NC       =6000   Yes No  |
| 3   0.0.0.0          0.0.0.0          ICMP  --       --      Yes Yes |
| 4   0.0.0.0          0.0.0.0          TCP   NC       >1023   Yes Yes |
| 5   0.0.0.0          0.0.0.0          UDP   NC       >1023   Yes Yes |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
+----------------------------------------------------------------------+
```

The table's columns correspond to each filter's attributes:

#: The filter's priority in the set. Filter number 1, with the highest priority, is first in the table.

Source IP Addr: The packet source IP address to match.

Dest IP Addr: The packet destination IP address to match.

Proto: The protocol to match. This can be entered as a number (see the table below) or as TCP or UDP if using those protocols.

Protocol	Number to use	Full name
N/A	0	Ignores protocol type
ICMP	1	Internet Control Message Protocol
TCP	6	Transmission Control Protocol
UDP	17	User Datagram Protocol

Src. Port: The source port to match. This is the port on the sending host that originated the packet.

D. Port: The destination port to match. This is the port on the receiving host for which the packet is intended.

On?: Displays **Yes** when the filter is in effect or **No** when it is not.

Fwd: Shows whether the filter forwards (**Yes**) a packet or discards (**No**) it when there's a match.

Filtering example #1

Returning to our filtering rule example from above (see page 14-7), look at how a rule is translated into a filter. Start with the rule, then fill in the filter's attributes:

1. The rule you want to implement as a filter is:

   Block all Telnet attempts that originate from the remote host 199.211.211.17.

2. The host 199.211.211.17 is the source of the Telnet packets you want to block, while the destination address is any IP address. How these IP addresses are masked determines what the final match will be, although the mask is not displayed in the table that displays the filter sets (you set it when you create the filter). In fact, since the mask for the destination IP address is 0.0.0.0, the address for Dest IP Addr could have been anything. The mask for Source IP Addr must be 255.255.255.255 since an exact match is desired.

   - Source IP Addr = 199.211.211.17
   - Source IP address mask = 255.255.255.255
   - Dest IP Addr = 0.0.0.0
   - Destination IP address mask = 0.0.0.0

   Note: To learn about IP addresses and masks, see Appendix C, "Understanding IP Addressing."

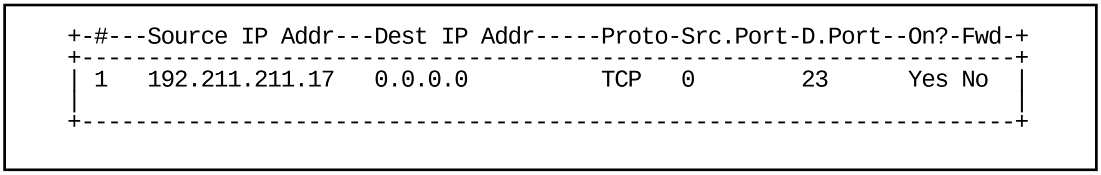
3. Using the tables on page 14-7, find the destination port and protocol numbers (the *local* Telnet port):

   - Proto = TCP (or 6)
   - D. Port = 23

4. The filter should be enabled and instructed to block the Telnet packets containing the source address shown in step 2:

   - On? = Yes
   - Fwd = No

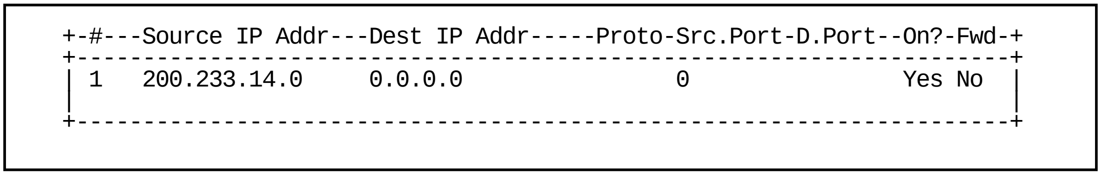
This four-step process is how we produced the following filter from the original rule:



```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+----------------------------------------------------------------------+
| 1   192.211.211.17   0.0.0.0          TCP    0        23      Yes No  |
|                                                                      |
+----------------------------------------------------------------------+
```

Filtering example #2

Suppose a filter is configured to block all incoming IP packets with the source IP address of 200.233.14.0, regardless of the type of connection or its destination. The filter would look like this:



```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+----------------------------------------------------------------------+
| 1   200.233.14.0     0.0.0.0                0                Yes No  |
|                                                                      |
+----------------------------------------------------------------------+
```

This filter blocks any packets coming from a remote network with the IP network address 200.233.14.0. The 0 at the end of the address signifies *any* host on the class C IP network 200.233.14.0. If, for example, the filter is applied to a packet with the source IP address 200.233.14.5, it will block it.

In this case, the mask, which does not appear in the table, must be set to 255.255.255.0. This way, all packets with a source address of 200.233.14.x will be matched correctly, no matter what the final address byte is.

Note: The protocol attribute for this filter is 0 by default. This tells the filter to ignore the IP protocol or type of IP packet.

Design guidelines

Careful thought should go into designing a new filter set. You should consider the following guidelines:

- Be sure the filter set's overall purpose is clear from the beginning. A vague purpose can lead to a faulty set, and that can actually make your network *less* secure.
- Be sure each individual filter's purpose is clear.
- Determine how filter priority will affect the set's actions. Test the set (on paper) by determining how the filters would respond to a number of different hypothetical packets.
- Consider the combined effect of the filters. If every filter in a set fails to match on a particular packet, the packet is:
  - passed if all the filters are configured to discard (*not* forward).
  - discarded if all the filters are configured to pass (forward).
  - discarded if the set contains a combination of pass and discard filters.

Disadvantages of filters

Although using filter sets can greatly enhance network security, there are disadvantages:

- Filters are complex. Combining them in filter sets introduces subtle interactions, increasing the likelihood of implementation errors.
- Enabling a large number of filters can have a negative impact on performance. Processing of packets will take longer if they have to go through many checkpoints.
- Too much reliance on packet filters can cause too little reliance on other security methods. Filter sets are *not* a substitute for password protection, effective safeguarding of passwords, caller ID, the "must match" option in the answer profile, PAP or CHAP in connection profiles, callback, and general awareness of how your network may be vulnerable.

An approach to using filters

The ultimate goal of network security is to prevent unauthorized access to the network without compromising authorized access. Using filter sets is part of reaching that goal.

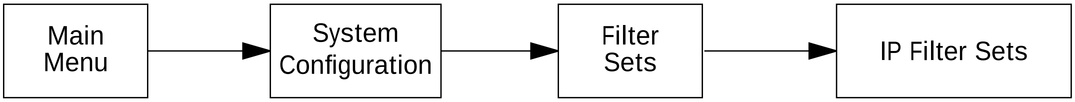
Each filter set you design will be based on one of the following approaches:

- That which is not expressly prohibited is permitted.
- That which is not expressly permitted is prohibited.

It is strongly recommended that you take the latter, and safer, approach to all of your filter set designs.

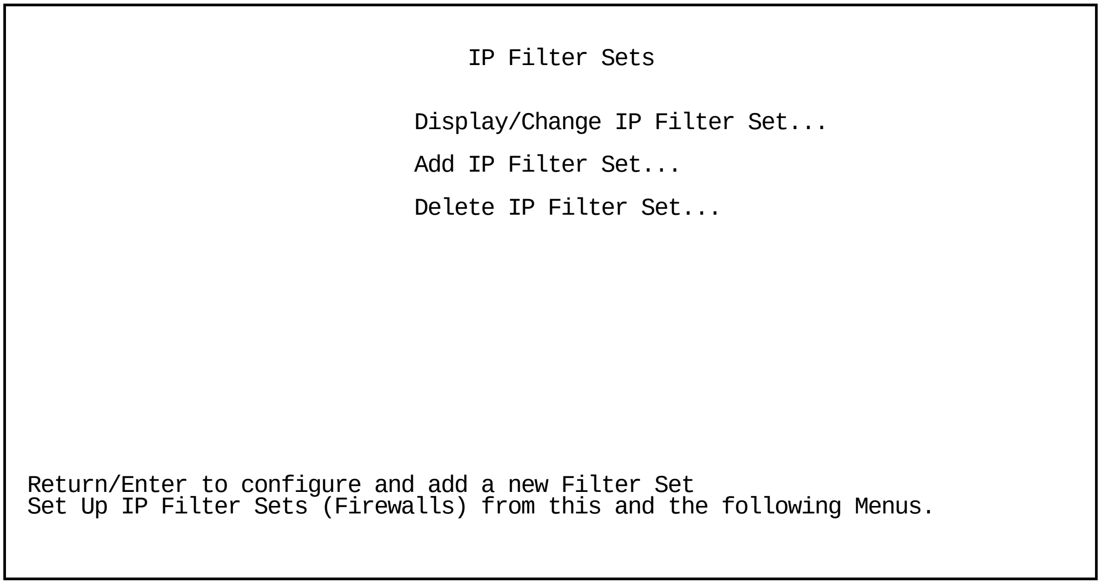
Working with IP filters and filter sets

This section covers IP filters and filter sets. For working with IPX filters and filter sets, see "IPX filters" on page 14-21.



To work with filters and filter sets, begin by accessing the filter set screens.

Note: Make sure you understand how filters work before attempting to use them. Read the section "About filters and filter sets," beginning on page 14-4.



```
                              IP Filter Sets

                          Display/Change IP Filter Set...
                          Add IP Filter Set...
                          Delete IP Filter Set...









Return/Enter to configure and add a new Filter Set
Set Up IP Filter Sets (Firewalls) from this and the following Menus.
```

The procedure for creating and maintaining filter sets is as follows:

1. Add a new filter set.
2. Create the filters for the new filter set.

3. View, change, or delete individual filters and filter sets.

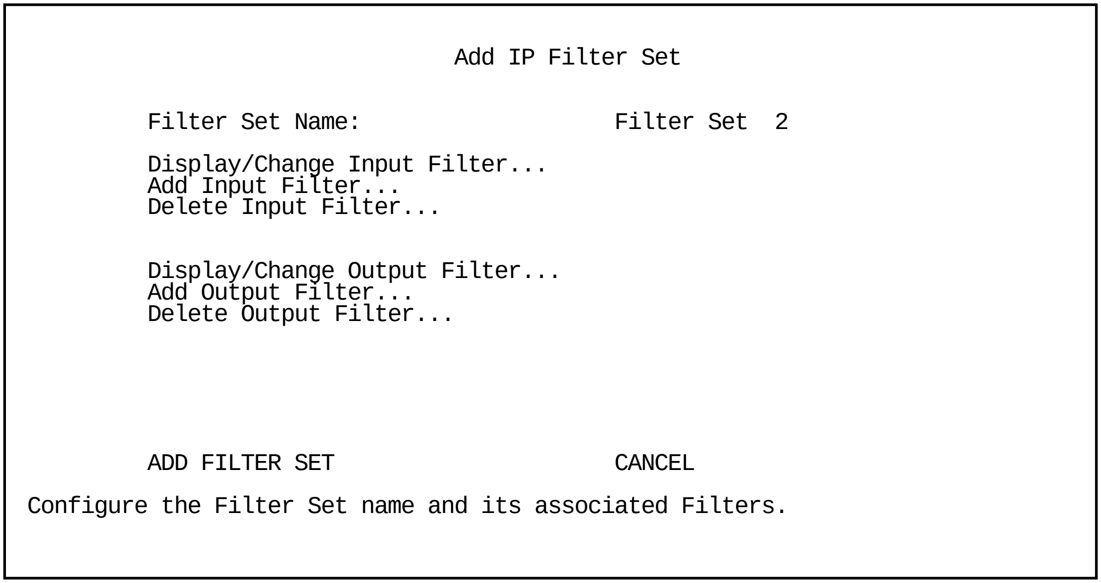
The sections below explain how to execute these steps.

Adding a filter set

You can create up to eight different custom filter sets. Each filter set can contain up to 16 output filters and up to 16 input filters.

To add a new filter set, select **Add IP Filter Set** in the IP Filter Sets screen and press Return to go to the Add Filter Set screen.

Note: There are two groups of items in the Add Filter Set screen, one for input filters and one for output filters. The two groups work in essentially the same way, as you'll see below.



```
                              Add IP Filter Set

         Filter Set Name:                  Filter Set  2

         Display/Change Input Filter...
         Add Input Filter...
         Delete Input Filter...


         Display/Change Output Filter...
         Add Output Filter...
         Delete Output Filter...





         ADD FILTER SET                    CANCEL

Configure the Filter Set name and its associated Filters.
```

Naming a new filter set

All new filter sets have a default name. The first filter set you add will be called Filter Set 1, the next filter will be Filter Set 2, and so on.

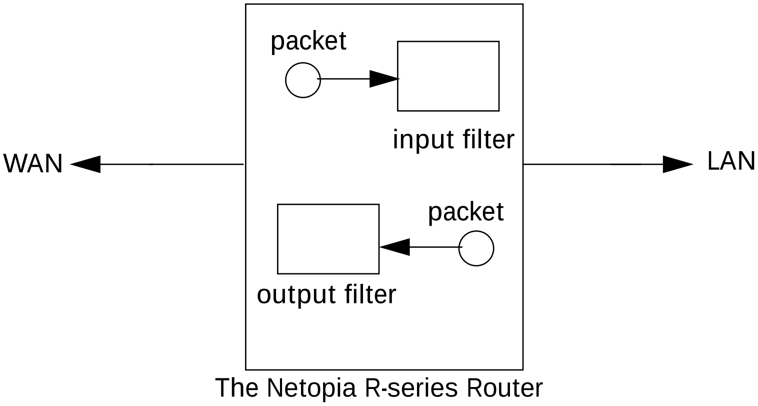
To give a new filter set a different name, select **Filter Set Name** and enter a new name for the filter set.

To save the filter set, select **ADD FILTER SET**. The saved filter set is empty (contains no filters), but you can return to it later to add filters (see "Modifying filter sets" on page 14-17). Or you can add filters to your new set before saving it (see "Adding filters to a filter set" on page 14-14).

Select **CANCEL** to leave the Add Filter Set screen without saving the new filter set and return to the Filter Sets screen.

Input and output filters—source and destination

There are two kinds of filters you can add to a filter set: input and output. Input filters check packets received from the Internet, destined for your network. Output filters check packets transmitted from your network to the Internet.



Packets in the Netopia R2020 pass through an input filter if they originate in the WAN and through an output filter if they're being sent out to the WAN.

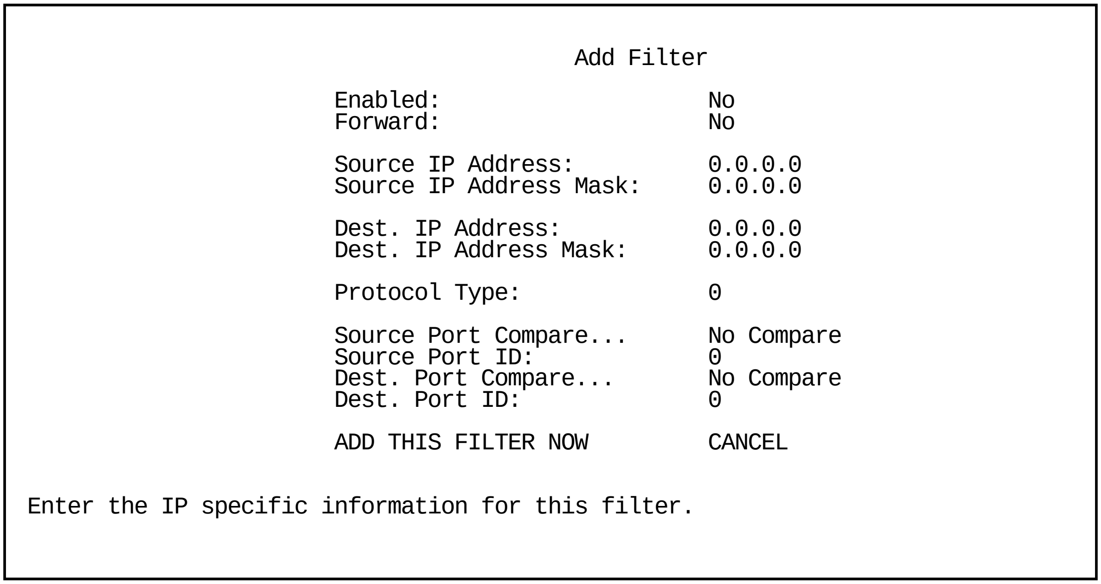
The process for adding input and output filters is exactly the same. The main difference between the two involves their reference to **source** and **destination**. From the perspective of an input filter, your local network is the **destination** of the packets it checks, and the remote network is their **source**. From the perspective of an output filter, your local network is the **source** of the packets, and the remote network is their **destination**.

Type of filter	"source" means	"destination" means
Input filter	the remote network	the local network
Output filter	the local network	the remote network

Adding filters to a filter set

In this section you'll learn how to add an input filter to a filter set. Adding an output filter works exactly the same way, providing you keep the different source and destination perspectives in mind.

To add an input filter, select **Add Input Filter** in the Add IP Filter Set screen and go to the Add Filter screen. (Select **Add Output Filter** to add an output filter.)



```
                                    Add Filter

                     Enabled:                      No
                     Forward:                      No

                     Source IP Address:            0.0.0.0
                     Source IP Address Mask:       0.0.0.0

                     Dest. IP Address:             0.0.0.0
                     Dest. IP Address Mask:        0.0.0.0

                     Protocol Type:                0

                     Source Port Compare...        No Compare
                     Source Port ID:               0
                     Dest. Port Compare...         No Compare
                     Dest. Port ID:                0

                     ADD THIS FILTER NOW           CANCEL


Enter the IP specific information for this filter.
```

1. To make the filter active in the filter set, select **Enabled** and toggle it to **Yes**. If **Enabled** is toggled to **No**, the filter can still exist in the filter set, but it will have no effect.

2. If you want the filter to forward packets that match its criteria to the destination IP address, select **Forward** and toggle it to **Yes**. If **Forward** is toggled to **No**, packets matching the filter's criteria will be discarded.

3. Select **Source IP Address** and enter the source IP address this filter will match on. You can enter a subnet or a host address.

4. Select **Source IP Address Mask** and enter a mask for the source IP address. This allows you to further modify the way the filter will match on the source address. Enter 0.0.0.0 to force the filter to match on all source IP addresses, or enter 255.255.255.255 to match the source IP address exclusively.

5. Select **Dest. IP Address** and enter the destination IP address this filter will match on. You can enter a subnet or a host address.

6. Select **Dest. IP Address Mask** and enter a mask for the destination IP address. This allows you to further modify the way the filter will match on the destination address. Enter 0.0.0.0 to force the filter to match on all destination IP addresses.

7. Select **Protocol Type** and enter **ICMP**, **TCP**, **UDP**, **Any**, or the number of another IP transport protocol (see the table on page 14-9).

   Note: If **Protocol Type** is set to **TCP** or **UDP**, the settings for port comparison that you configure in steps 8 and 9 will appear. These settings only take effect if the Protocol Type is TCP or UDP.

8. Select **Source Port Compare** and choose a comparison method for the filter to use on a packet's source port number. Then select **Source Port ID** and enter the actual source port number to match on (see the table on page 14-7).

9. Select **Dest. Port Compare** and choose a comparison method for the filter to use on a packet's destination port number. Then select **Dest. Port ID** and enter the actual destination port number to match on (see the table on page 14-7).

10. When you are finished configuring the filter, select **ADD THIS FILTER NOW** to save the filter in the filter set. Select **CANCEL** to discard the filter.

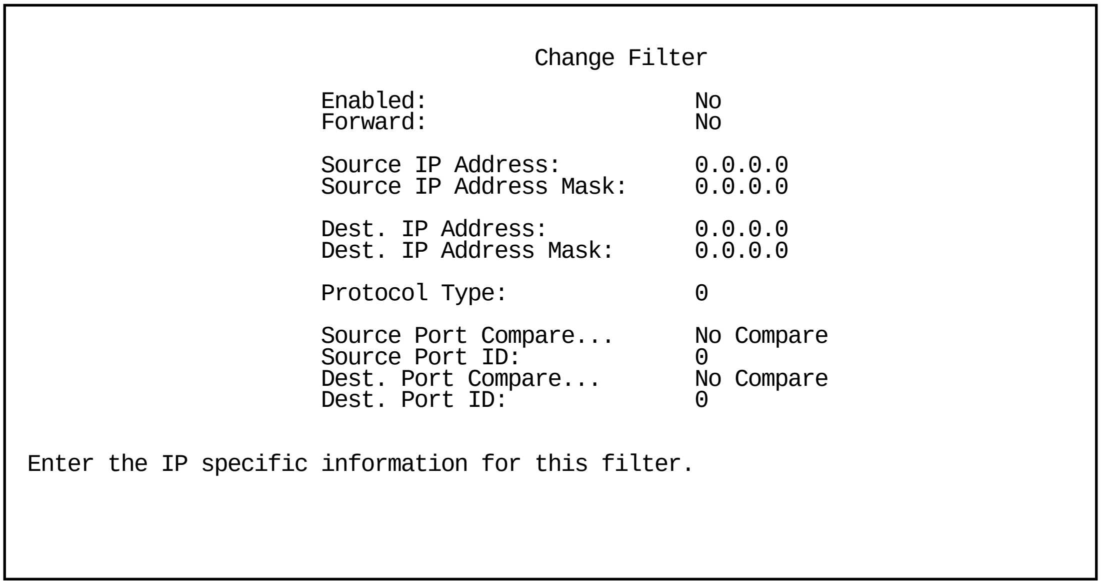
Viewing filters

To display a view-only table of input (output) filters, select **Display / Change Input Filters** (**Display / Change Output Filters**) in the Add IP Filter Set screen.

Modifying filters

To modify a filter, select **Display / Change Input Filter** (**Display / Change Output Filter**) in the Add IP Filter Set screen to display a table of filters.

Select a filter from the table and press Return to go to the Change Filter screen. The parameters in this screen are the same as the ones in the Add Filter screen (see “Adding filters to a filter set” on page 14-14).



```
                                Change Filter

                      Enabled:                      No
                      Forward:                      No

                      Source IP Address:            0.0.0.0
                      Source IP Address Mask:       0.0.0.0

                      Dest. IP Address:             0.0.0.0
                      Dest. IP Address Mask:        0.0.0.0

                      Protocol Type:                0

                      Source Port Compare...        No Compare
                      Source Port ID:               0
                      Dest. Port Compare...         No Compare
                      Dest. Port ID:                0


Enter the IP specific information for this filter.
```

Deleting filters

To delete a filter, select **Delete Input Filter** (**Delete Output Filter**) in the Add Filter Set screen to display a table of filters.

Select the filter from the table and press Return to delete it. Press the Escape key to exit the table without deleting the filter.

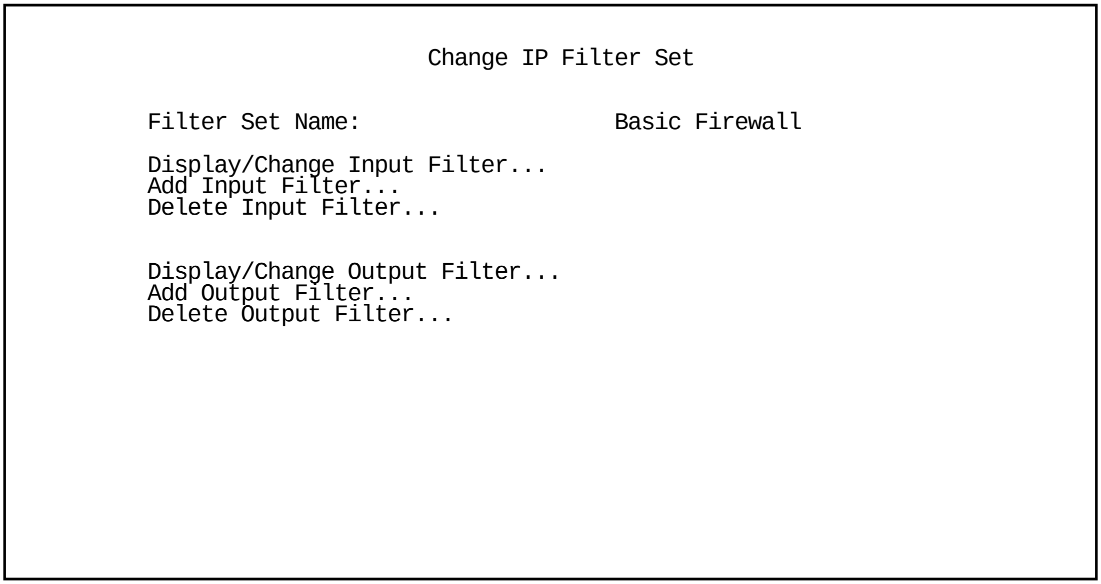
Viewing filter sets

To display a view-only list of filter sets, select **Display / Change Filter Sets** in the IP Filter Sets screen.

Modifying filter sets

To modify a filter set, select **Display / Change Filter Set** in the Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to go to the Change IP Filter Set screen. The items in this screen are the same as the ones in the Add Filter screen (see “Adding filters to a filter set” on page 14-14).



```
                              Change IP Filter Set

          Filter Set Name:                      Basic Firewall

          Display/Change Input Filter...
          Add Input Filter...
          Delete Input Filter...


          Display/Change Output Filter...
          Add Output Filter...
          Delete Output Filter...
```

Deleting a filter set

Note: If you delete a filter set, all of the filters it contains are deleted as well. To reuse any of these filters in another set, you’ll have to note their configuration before deleting the current filter set and then recreate them.

To delete a filter set, select **Delete Filter Set** in the IP Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to delete it. Press the Escape key to exit the list without deleting the filter set.

A sample IP filter set

This section contains the settings for a filter set, called Basic Firewall, which is part of the Netopia R2020’s factory configuration.

Basic Firewall blocks undesirable traffic originating from the WAN (in most cases, the Internet), but passes all traffic originating from the LAN. It follows the conservative “that which is not expressly permitted is prohibited” approach: unless an incoming packet expressly matches one of the constituent input filters, it will not be forwarded to the LAN.

The five input filters and one output filter that make up Basic Firewall are shown in the table below.

Setting	Input filter 1	Input filter 2	Input filter 3	Input filter 4	Input filter 5	Output filter 1
Enabled	Yes	Yes	Yes	Yes	Yes	Yes
Forward	No	No	Yes	Yes	Yes	Yes
Source IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Source IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Protocol type	TCP	TCP	ICMP	TCP	UDP	0
Source port comparison	No Compare	No Compare	N/A	No Compare	No Compare	N/A
Source port ID	0	0	N/A	0	0	N/A
Dest. port comparison	Equal	Equal	N/A	Greater Than	Greater Than	N/A
Dest. port ID	2000	6000	N/A	1023	1023	N/A

Basic Firewall's filters play the following roles.

Input filters 1 and 2: These block WAN-originated OpenWindows and X-Windows sessions. Service origination requests for these protocols use ports 2000 and 6000, respectively. Since these are greater than 1023, OpenWindows and X-Windows traffic would otherwise be allowed by input filter 4. Input filters 1 and 2 must precede input filter 4; otherwise they would have no effect as filter 4 would have already passed OpenWindows and X-Windows traffic.

Input filter 3: This filter explicitly passes all WAN-originated ICMP traffic to permit devices on the WAN to ping devices on the LAN. Ping is an Internet service that is useful for diagnostic purposes.

Input filters 4 and 5: These filters pass all TCP and UDP traffic, respectively, when the destination port is greater than 1023. This type of traffic generally does not allow a remote host to connect to the LAN using one of the potentially intrusive Internet services, such as Telnet, FTP, and WWW.

Output filter 1: This filter passes all outgoing traffic to make sure that no outgoing connections from the LAN are blocked.

Basic Firewall is suitable for a LAN containing only client hosts that wish to access servers on the WAN, not for a LAN containing servers providing services to clients on the WAN. Basic Firewall's general strategy is to explicitly pass WAN-originated TCP and UDP traffic to ports greater than 1023. Ports lower than 1024 are the service origination ports for various Internet services such as FTP, Telnet, and the World Wide Web (WWW).

A more complicated filter set would be required to provide WAN access to a LAN-based server. See "Possible modifications," below, for ways to allow remote hosts to use services provided by servers on the LAN.

Possible modifications

You can modify the sample filter set Basic Firewall to allow incoming traffic using the examples below. These modifications are not intended to be combined. Each modification is to be the only one used with Basic Firewall.

The results of combining filter set modifications can be difficult to predict. It is recommended that you take special care if making more than one modification to the sample filter set.

Trusted host. To allow unlimited access by a trusted remote host with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

Trusted subnet. To allow unlimited access by a trusted remote subnet with subnet address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.0) and subnet mask e.f.g.h (corresponding to a numbered IP mask such as 255.255.255.0), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: e.f.g.h
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

FTP sessions. To allow WAN-originated FTP sessions to a LAN-based FTP server with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

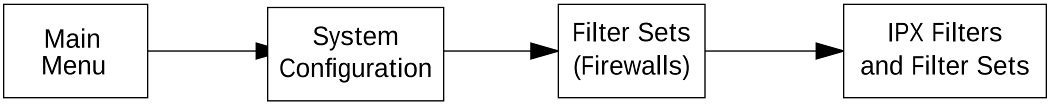
- Enabled: Yes
- Forward: Yes
- Source IP Address: 0.0.0.0
- Source IP Address Mask: 0.0.0.0
- Dest. IP Address: a.b.c.d
- Dest. IP Address Mask: 255.255.255.255
- Protocol Type: TCP
- Source Port Comparison: No Compare
- Source Port ID: 0
- Dest. Port Comparison: Equal
- Dest. Port ID: 21

Note: A similar filter could be used to permit Telnet or WWW access. Set the Dest. Port ID to 23 for Telnet or 80 for WWW.

AURP tunnel. To allow an AURP tunnel between a remote AURP router with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243) and a local AURP router (including the Netopia R2020 itself), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: UDP
- Source Port Comparison: Equal
- Source Port ID: 387
- Dest. Port Comparison: Equal
- Dest. Port ID: 387

IPX filters



IPX packet filters work very similarly to IP packet filters. They filter data traffic coming from or going to remote IPX networks. IPX filters can be set up to pass or discard IPX packets based on a number of user-defined criteria. Like IP filters, IPX filters must be grouped in sets that are applied to the answer profile or to connection profiles.

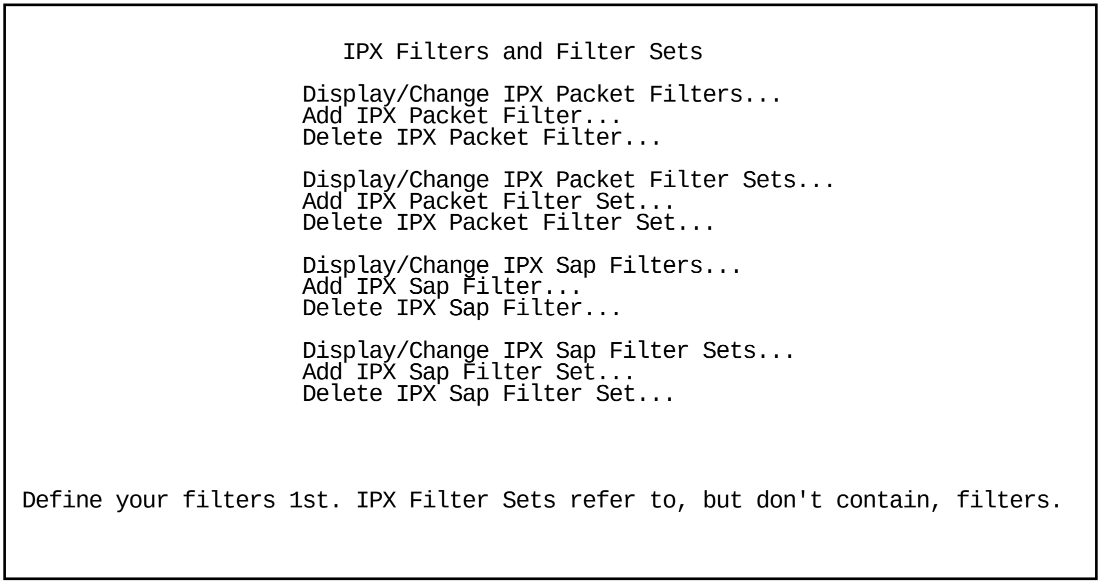
IPX SAP filters are used for filtering server entries not required to pass over the WAN links. When connecting to a large IPX network via dial-up connection, the transfer of large numbers of SAP entries can consume significant bandwidth on the WAN link.

Note: Using SAP filtering to prevent a server from being advertised does not provide security against that server being accessed—IPX packet filtering must be used for that purpose.

Setting up and using IPX filter sets is a four-step process:

1. Create the filters to use.
2. Create the filter sets to use.
3. Add filters to the filter sets.
4. Attach the filter sets to the answer profile or to connection profiles.

You can configure IPX filters and set up IPX filter sets from the IPX Filters and Filter Sets screen.


```
                    IPX Filters and Filter Sets

                 Display/Change IPX Packet Filters...
                 Add IPX Packet Filter...
                 Delete IPX Packet Filter...

                 Display/Change IPX Packet Filter Sets...
                 Add IPX Packet Filter Set...
                 Delete IPX Packet Filter Set...

                 Display/Change IPX Sap Filters...
                 Add IPX Sap Filter...
                 Delete IPX Sap Filter...

                 Display/Change IPX Sap Filter Sets...
                 Add IPX Sap Filter Set...
                 Delete IPX Sap Filter Set...



Define your filters 1st. IPX Filter Sets refer to, but don't contain, filters.
```

The items in the IPX Filters and Filter Sets screen are grouped into four areas:

- IPX packet filters
- IPX packet filter sets
- IPX SAP filters
- IPX SAP filter sets

The following sections explain the items in each of these areas.

IPX packet filters

For each IPX packet filter, you can configure a set of parameters to match on the source or destination attributes of IPX data packets coming from or going to the WAN.

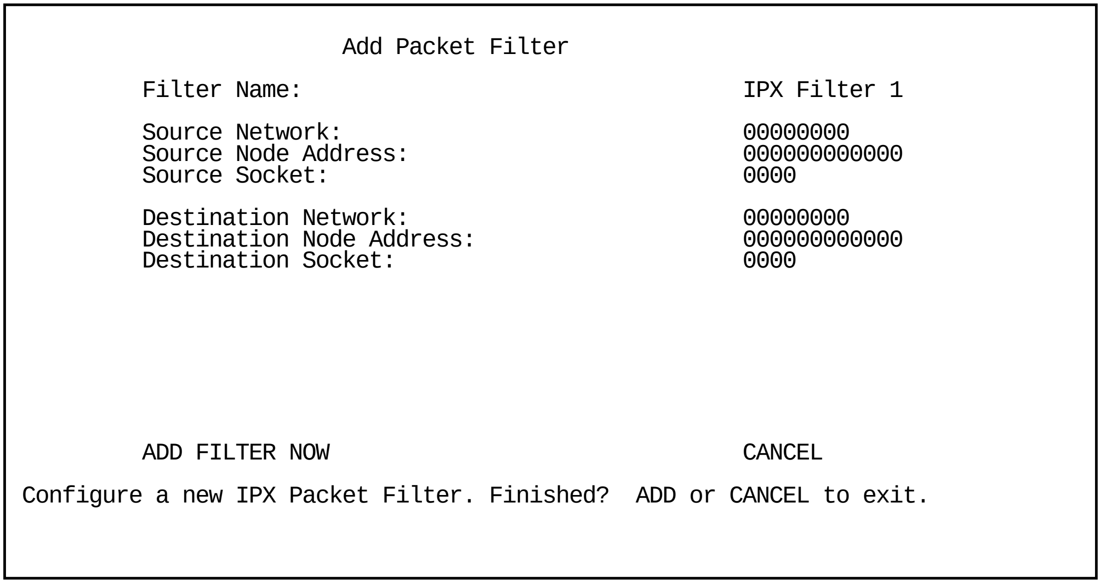
Viewing and modifying packet filters

To display a view-only table of IPX packet filters, select **Show / Change IPX Packet Filters** in the IPX Filters and Filter Sets screen.

To modify any of the filters in the table, note the desired filter and press Return to go to the Change Packet Filter screen. The parameters in this screen are the same as the ones in the Add Packet Filter screen (see the next section).

Adding a packet filter

To add a new IPX packet filter, select **Add IPX Packet Filter** in the IPX Filters and Filter Sets screen and press Return to go to the Add Packet Filter screen.



```
                         Add Packet Filter

          Filter Name:                                 IPX Filter 1

          Source Network:                              00000000
          Source Node Address:                         000000000000
          Source Socket:                               0000

          Destination Network:                         00000000
          Destination Node Address:                    000000000000
          Destination Socket:                          0000






          ADD FILTER NOW                               CANCEL

 Configure a new IPX Packet Filter. Finished?  ADD or CANCEL to exit.
```

By default, the filter's socket numbers and network and node addresses are null (all zeros). This sets the filter to match on any IPX data packet. You should configure the filter using criteria that meet your security needs.

1. Select **Filter Name** and enter a descriptive name for the filter.
2. To specify a source network for the filter to match on, select **Source Network** and enter an IPX network address.
3. To specify a source node for the filter to match on, select **Source Node Address** and enter an IPX node address.
4. To specify a source socket for the filter to match on, select **Source Socket** and enter an IPX source socket number.
5. To specify a destination network for the filter to match on, select **Destination Network** and enter an IPX network address.
6. To specify a destination node for the filter to match on, select **Destination Node Address** and enter an IPX node address.
7. To specify a destination socket for the filter to match on, select **Destination Socket** and enter an IPX destination socket number.
8. Select **ADD FILTER NOW** to save the current filter. Select **CANCEL** to exit the Add Packet Filter screen without saving the new filter.

Deleting a packet filter

To delete a packet filter, select **Delete IPX Packet Filter** in the IPX Filters and Filter Sets screen to display a table of filters. Select a filter from the table and press Return to delete it. Press the Escape key to exit the table without deleting the filter.

IPX packet filter sets

Before the individual filters can be used, IPX packet filters must be grouped into sets. A filter can be part of more than one filter set.

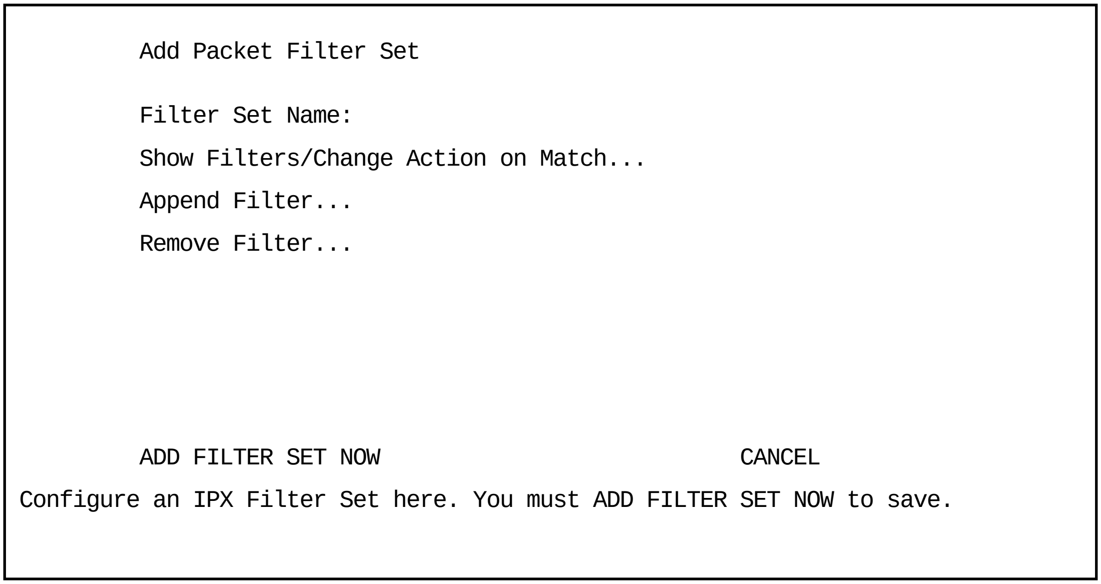
Viewing and modifying packet filter sets

To display a table of IPX packet filter sets, select **Show/Change IPX Packet Filter Sets** in the IPX Filters and Filter Sets screen.

To modify any of the filter sets in the list, select the desired filter set and press Return to go to the Change Packet Filter Set screen. The parameters in this screen are the same as the ones in the Add Packet Filter Set screen (see the next section).

Adding a packet filter set

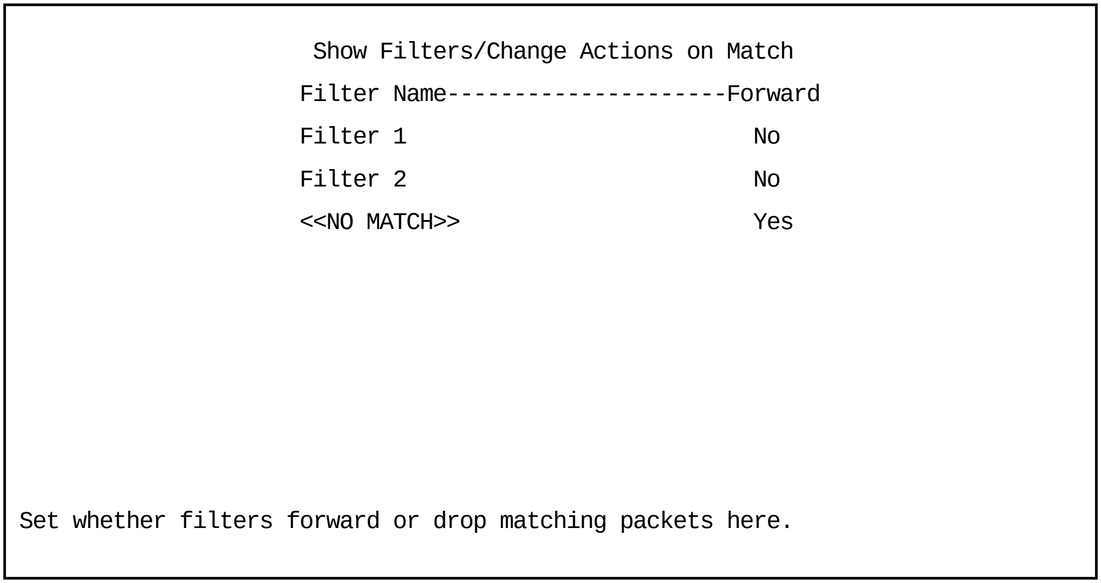
To add a new IPX packet filter set, select **Add IPX Packet Filter Set** in the IPX Filters and Filter Sets screen and press Return to go to the Add Packet Filter Set screen.



```
         Add Packet Filter Set

         Filter Set Name:

         Show Filters/Change Action on Match...

         Append Filter...

         Remove Filter...




         ADD FILTER SET NOW                           CANCEL

Configure an IPX Filter Set here. You must ADD FILTER SET NOW to save.
```

Follow these steps to configure the new packet filter set:

1. Select **Filter Set Name** and enter a descriptive name for the filter set.
2. To change the forwarding action of filters in the filter set, select **Show Filters / Change Action on Match** and press Return to go to the Show Filters / Change Actions on Match screen.



```
                    Show Filters/Change Actions on Match

                   Filter Name---------------------Forward

                   Filter 1                          No

                   Filter 2                          No

                   <<NO MATCH>>                      Yes




Set whether filters forward or drop matching packets here.
```

Select a filter and toggle the packet forwarding action to **Yes** (pass) or **No** (discard).

3. To add a filter to the filter set, select **Append Filter** to display a table of filters. Select a filter from the table and press Return to add it to the filter set. The default action of newly added filters is to *not* forward packets that match their criteria.

   To exit the table without adding the filter, press the Escape key.

4. To remove a filter from the filter set, select **Detach Filter** to display a table of appended filters. Select a filter from the table and press Return to remove it from the set. To exit the table without removing the filter, press the Escape key.

5. Select **ADD FILTER SET NOW** to save the current filter set. Select **CANCEL** to exit the Add Packet Filter Set screen without saving the new filter set.

Deleting a packet filter set

To delete a packet filter set, select **Delete IPX Packet Filter Set** in the IPX Filters and Filter Sets screen to display a list of filter sets. Select a filter set from the list and press Return to delete it. Press the Escape key to exit the list without deleting the filter set.

Note: Deleting a filter set does not delete the filters in that set. However, the filters in the deleted set are no longer in effect (unless they are part of another set). The deleted set will no longer appear in the answer profile or any connection profiles to which it was added.

IPX SAP filters

For each IPX SAP filter, you can configure a set of parameters to match on certain attributes of IPX SAP packet entries. The filters check IPX SAP packets for entries that match and then act on those entries. The SAP packets themselves are always allowed to continue after their entries are checked.

The purpose of filtering SAP packets is not to make your network more secure, but to add efficiency to network bandwidth use. Filtering SAP packets may reduce the size of SAP packets and SAP bindery tables by removing unwanted entries.

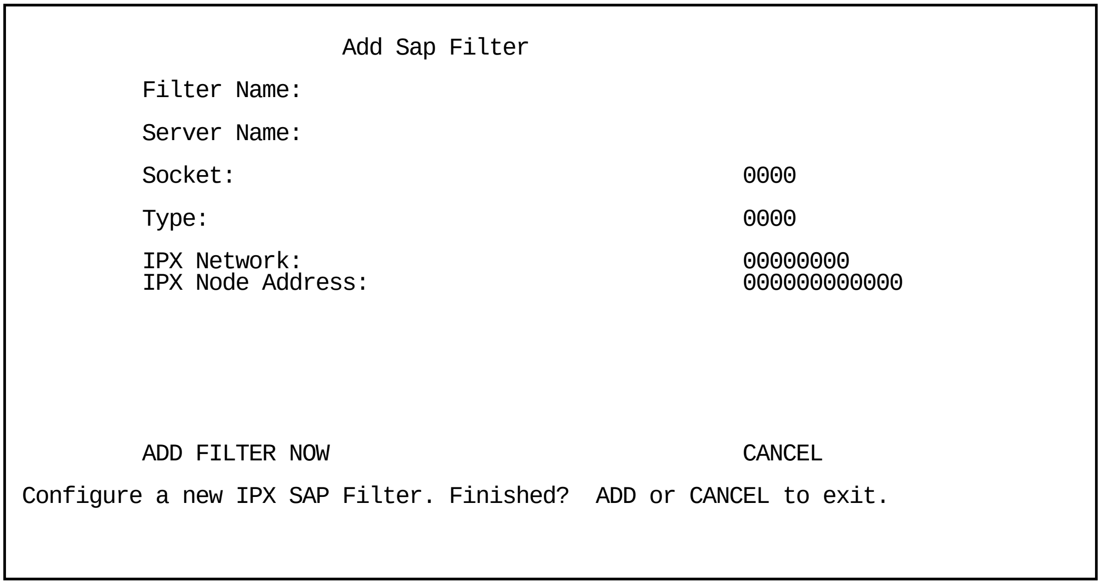
Viewing and modifying SAP filters

To display a table of IPX SAP filters, select **Show/Change IPX SAP Filters** in the IPX Filters and Filter Sets screen.

To modify any of the filters in the table, select the desired filter and press Return to go to the Change SAP Filter screen. The parameters in this screen are the same as the ones in the Add SAP Filter screen (see the next section).

Adding a SAP filter

To add a new IPX SAP filter, select **Add IPX SAP Filter** in the IPX Filters and Filter Sets screen and press Return to go to the Add SAP Filter screen.



```
                      Add Sap Filter

         Filter Name:

         Server Name:

         Socket:                                      0000

         Type:                                        0000

         IPX Network:                                 00000000
         IPX Node Address:                            000000000000





         ADD FILTER NOW                               CANCEL

Configure a new IPX SAP Filter. Finished?  ADD or CANCEL to exit.
```

By default, the filter’s socket and type numbers and network and node addresses are null (all zeros). This sets the filter to match on any IPX SAP packet entry. You should configure the filter using criteria that meet your needs.

Follow these steps to configure the new SAP filter:

1. Select **Filter Name** and enter a descriptive name for the filter.
2. To specify a server name for the filter to match on, select **Server Name** and enter the name of an IPX server. You can use the wildcard characters * (asterisk) and ? (question mark). Use * to match any string, including a null string (no characters), and ? to match any single character in the server’s name. For example, the filter could match on the server name “NETOPIA” with “NETO*”, “NETO?IA”, and “NETOPIA*”.
3. To specify a socket for the filter to match on, select **Socket** and enter an IPX socket number.
4. To specify a type number for the filter to match on, select **Type** and enter an IPX type number.
5. To specify an IPX network address for the filter to match on, select **IPX Network** and enter an IPX network address.
6. To specify an IPX node address for the filter to match on, select **IPX Node Address** and enter an IPX node address.
7. Select **ADD FILTER NOW** to save the current filter. Select **CANCEL** to exit the Add SAP Filter screen without saving the new filter.

Deleting a SAP filter

To delete a SAP filter, select **Delete IPX SAP filter** in the IPX Filters and Filter Sets screen to display a table of filters. Select a filter from the table and press Return to delete it. Press the Escape key to exit the table without deleting the filter.

IPX SAP filter sets

Before IPX SAP filters can be used, they must be grouped into sets. A SAP filter can be part of more than one filter set.

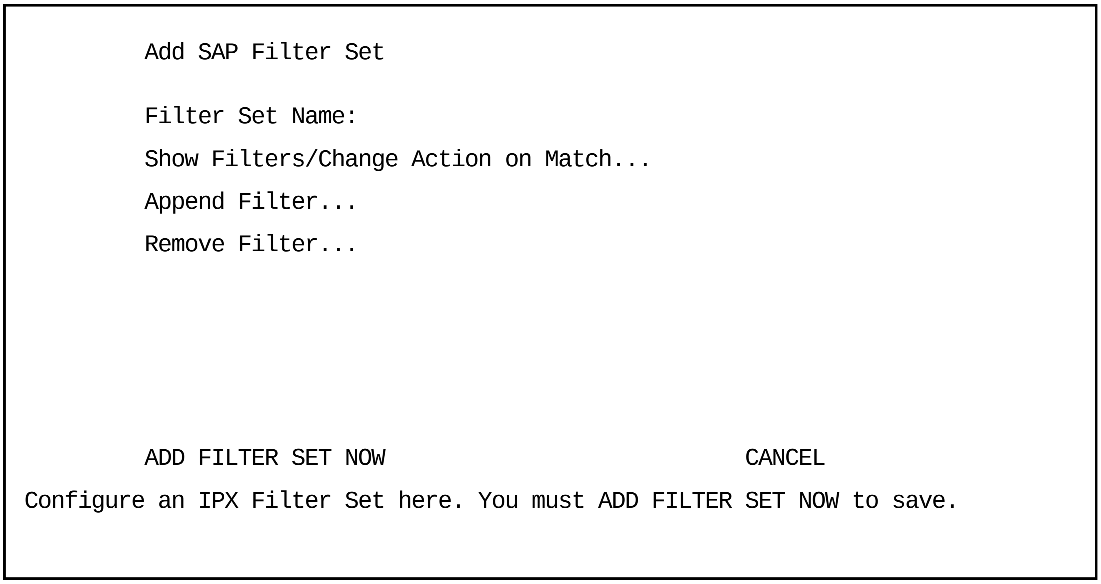
Viewing and modifying SAP filter sets

To display a table of IPX SAP filter sets, select **Show / Change IPX SAP Filter Sets** in the IPX Filters and Filter Sets screen to display a list of filter sets.

To modify any of the filter sets in the list, select the desired filter set and go to the Change SAP Filter Set screen. The parameters in this screen are the same as the ones in the Add SAP Filter Set screen (see the previous section).

Adding a SAP filter set

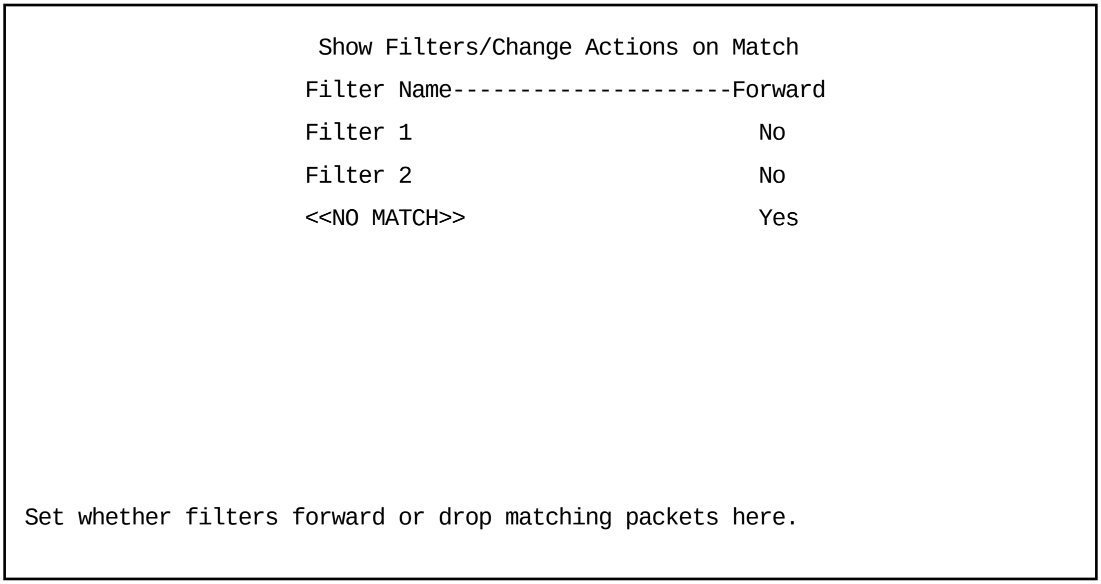
To add a new IPX SAP filter set, select **Add IPX SAP Filter Set** in the IPX Filters and Filter Sets screen and go to the Add SAP Filter Set screen.



```
          Add SAP Filter Set

          Filter Set Name:

          Show Filters/Change Action on Match...

          Append Filter...

          Remove Filter...






          ADD FILTER SET NOW                          CANCEL

Configure an IPX Filter Set here. You must ADD FILTER SET NOW to save.
```

Follow these steps to configure the new SAP filter set:

1. Select **Filter Set Name** and enter a descriptive name for the filter set.
2. To change the forwarding action of filters in the filter set, select **Show Filters / Change Action on Match** and press Return to go to the Show Filters / Change Actions on Match screen.



```
                     Show Filters/Change Actions on Match
                    Filter Name---------------------Forward
                    Filter 1                          No
                    Filter 2                          No
                    <<NO MATCH>>                      Yes









Set whether filters forward or drop matching packets here.
```

Select a filter and toggle the entry forwarding action to **Yes** (pass) or **No** (discard).

3. To add a filter to the filter set, select **Append Filter** to display a table of filters. Select a filter from the table and press Return to add it to the filter set. The default action of newly added filters is to *not* forward (discard) packet entries that match their criteria.

   To exit the table without adding the filter, press the Escape key.

4. To remove a filter from the filter set, select **Detach Filter** to display a table of appended filters. Select a filter from the table and press Return to remove it from the set. To exit the table without removing the filter, press the Escape key.

5. Select **ADD FILTER SET NOW** to save the current filter set. Select **CANCEL** to exit the Add SAP Filter Set screen without saving the new filter set.

Deleting a SAP filter set

To delete a SAP filter set, select **Delete IPX SAP Filter Set** in the IPX Filters and Filter Sets screen to display a list of filter sets. Select a filter set from the list and press Return to delete it. Press the Escape key to exit the list without deleting the filter set.

Note: Deleting a filter set does not delete the filters in that set. However, the filters in the deleted set are no longer in effect (unless they are part of another set). The deleted set will no longer appear in the answer profile or any connection profiles to which it was added.

Firewall tutorial

General Firewall Terms

Firewall: a component or set of components that restrict access between a protected network and the Internet, or between two networks.

Host: A workstation on the Network.

Packet: Unit of communication on the Internet.

Packet Filter: Packet filters allow or deny packets based on source or destination IP addresses, TCP or UDP ports, or the TCP ACK bit.

Port: A number that defines a particular type of service.

Filter Rule: A filter set is comprised of individual filter rules.

Filter Set: A grouping of individual filter rules.

Basic IP Packet Components

All IP packets contain the same basic “header” information, as follows:

Source IP Address	163.176.132.18
Destination IP Address	163.176.4.27
Source Port	2541
Destination Port	80
Protocol	TCP
ACK Bit	Yes
DATA	User Data

This header information is what the packet filter uses to make filtering decisions. It is important to note that a packet filter does not look into the IP datastream (the User Data from above) to make filtering decisions.

Basic Protocol Types

TCP: Transmission Control Protocol. TCP provides reliable packet delivery and has a retransmission mechanism (so packets are not lost). RFC 793 is the specification for TCP.

UDP: User Datagram Protocol. Unlike TCP, UDP does not guarantee reliable, sequenced packet delivery. If data does not reach its destination, UDP does not re transmit the data. RFC 768 is the specification for UDP.

And there are many more ports defined in the Assigned Addresses RFC.

Example TCP/UDP Ports

TCP Port	Service	UDP Port	Service
20/21	FTP	161	SNMP
23	Telnet	69	TFTP
25	SMTP	387	AURP

80	WWW		
144	News		

Firewall design rules

There are two basic rules to firewall design:

- "What is not explicitly allowed is denied..."

and

- "What is not explicitly denied is allowed..."

The first rule is far more secure, and is the best approach to firewall design. It is far easier (and more secure) to allow in or out only certain services and deny anything else. If the other rule is used, you would have to figure out everything that you want to disallow, now and future.

Firewall Logic

Firewall design is a test of logic, and filter rule ordering is critical. If a packet is passed through a series of filter rules and then the packet matches a rule, the appropriate action is taken. The packet will not pass through the remainder of the filter rules.

For example, if you had the following filter set...

Allow WWW access;

Allow FTP access;

Allow SMTP access;

Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would pass through the first rule (WWW), go through the second rule (FTP), matches this rule and the packet is allowed through.

If you had this filter set for example....

Allow WWW access;

Allow FTP access;

Deny FTP access;

Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would pass through the first filter rule (WWW), match the second rule (FTP) and the packet is allowed through. Even though the next rule is to deny all FTP traffic, the FTP packet will never make it to this rule.

Binary Representation

It is easiest when doing filtering to convert the IP address and mask in question to binary. This will allow you to perform the logical AND to determine if a packet matches a filter rule.

Logical ANDing

When a packet is compared (in most cases) a logical AND is performed. First the IP addresses and subnet masks are converted to binary and then ANDed together. The rules for logical ANDing are as follows:

0 AND 0 = 0

0 AND 1 = 0

1 AND 0 = 0

1 AND 1 = 1

For example:

Filter rule:

Deny

IP: 163.176.1.15 BINARY: 10100011.10110000.00000001.00001111

Mask: 255.255.255.255 BINARY: 11111111.11111111.11111111.11111111

Incoming Packet:

IP 163.176.1.15 BINARY: 10100011.10110000.00000001.00001111

AND the incoming packet and subnet mask together, the result is:

10100011.10110000.00000001.00001111

which matches the IP address in the filter rule and the packet is denied.

Implied Rules

With a given set of filter rules, there is an Implied rule which may or may not be shown to the user. The implied rule tells the filter set what to do with a packet that does not match any of the filter rules. An example of implied rules is as follows:

Implied	Meaning
Y+Y+Y=N	If all filter rules are YES, the implied is NO.
N+N+N=Y	If all filter rules are NO, the implied is YES.
Y+N+Y=N	If a mix of YES and NO filters, the implied is NO.

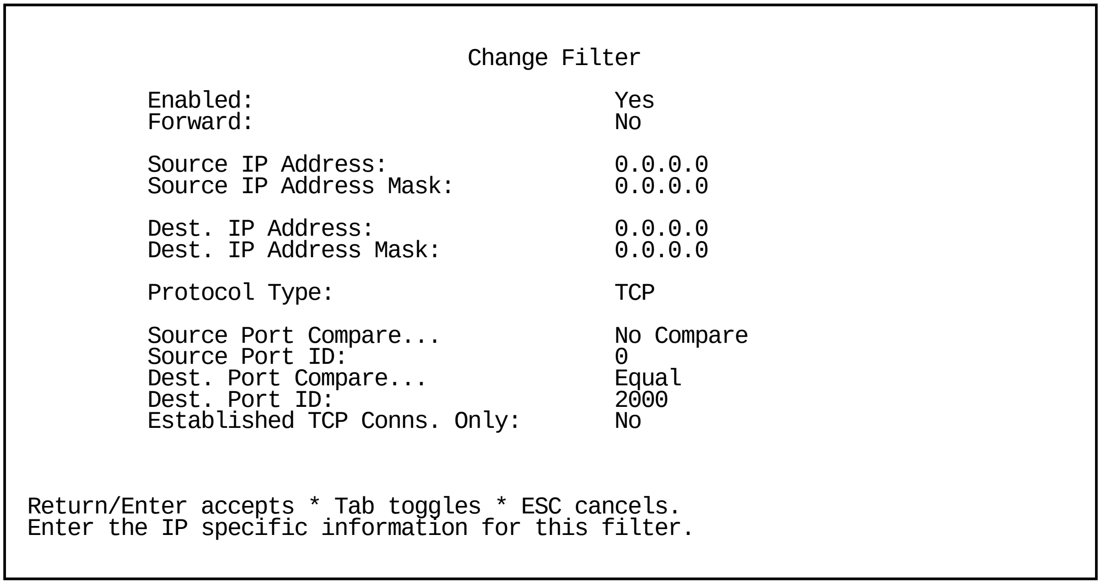
Established Connections

The TCP header contains one bit called the ACK Bit (or TCP Ack bit). This ACK Bit only appears with TCP, not UDP. The ACK bit is part of the TCP mechanism that guaranteed the delivery of data. The ACK bit is set whenever one side of a connection has received data from the other side. Only the first TCP packet will not have the ACK bit set, once the TCP connection is in place the remainder of the TCP packets with have the ACK bit set.

The ACK bit is helpful for firewall design and reduces the number of potential filter rules. A filter rule could be created just allowing incoming TCP packets with the ACK bit set, as these packets had to be originated from the local network.

Example IP Filter Set Screen

This is an example of the Netopia IP filter set screen:



```
                                   Change Filter

         Enabled:                                  Yes
         Forward:                                  No

         Source IP Address:                        0.0.0.0
         Source IP Address Mask:                   0.0.0.0

         Dest. IP Address:                         0.0.0.0
         Dest. IP Address Mask:                    0.0.0.0

         Protocol Type:                            TCP

         Source Port Compare...                    No Compare
         Source Port ID:                           0
         Dest. Port Compare...                     Equal
         Dest. Port ID:                            2000
         Established TCP Conns. Only:              No


Return/Enter accepts * Tab toggles * ESC cancels.
Enter the IP specific information for this filter.
```

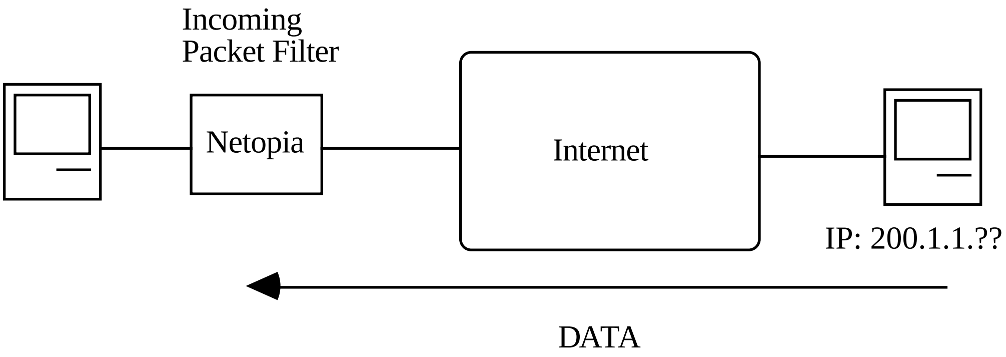
Filter Basics

In the source or destination IP address fields, the IP address that is entered MUST be the NETWORK address of the subnet. A HOST address can be entered, but the applied subnet mask must be 32 bits (255.255.255.255).

The Netopia R2020 has the ability to compare source and destination TCP or UDP ports. These options are as follows:

Item	What it means
No compare	Does not compare TCP or UDP port
Not Equal To	Matches any port other than what is defined
Less Than	Anything less than the port defined
Less Than Or Equal	Any port less than or equal to the port defined
Equal	Matches only the port defined
Greater Than or Equal	Matches the port or any port greater
Greater Than	Matches anything greater than the port defined.

Example Network



Example Filters

Example 1

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.28

IP Address	Binary Representation	
200.1.1.28	00011100	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	00000000	(Logical AND result)

This incoming IP packet has a source IP address that matches the network address in the Source IP Address field (00000000) in the Netopia R2020. This will NOT forward this packet.

Example 2

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	10000000	(Logical AND result)

This incoming IP packet (10000000) has a source IP address that does not match the network address in the Source IP Address field (00000000) in the Netopia R2020. This rule WILL forward this packet because the packet does not match.

Example 3

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	10110000	(Logical AND result)

Since the Source IP Network Address in the Netopia R2020 is 01100000, and the source IP address after the logical AND is 1011000, this rule does NOT match and this packet will be passed.

Example 4

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.104

IP Address	Binary Representation	
200.1.1.104	01101000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia R2020 is 01100000, and the source IP address after the logical AND is 01100000, this rule DOES match and this packet will NOT be passed.

Example 5

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.255	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.96

IP Address	Binary Representation	
200.1.1.96	01100000	(Source address in incoming IP packet)
AND		
255.255.255.255	11111111	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia R2020 is 01100000, and the source IP address after the logical AND is 01100000, this rule DOES match and this packet will NOT be passed. This rule masks off a SINGLE IP address.

Token Security Authentication

This section discusses how to configure and use security authentication on the Netopia R2020.

Note: The security authentication feature only applies to Netopia R2020 models connecting over a dial-up line using the PPP-PAP-TOKEN or PPP-CACHE-TOKEN authentication protocol.

Securing network environments

Unauthorized tampering or theft of information on internal networks causes serious ramifications, given the reliance on information systems. Network abuse is a serious problem, complicated by the difficulty in detecting the source of the abuses. An unauthorized user can gain access to networks and copy information without leaving a trace.

Password protection is one solution, but static passwords are often insecure. They can be compromised, allowing unauthorized users to disguise themselves as authorized users and enter supposedly secure systems. However, a company called Security Dynamics™ has patented a security authentication technology to increase network security.

SecurID is a two-factor authentication process to protect against unauthorized access. This dynamic user authentication produces a randomly-generated security code mechanism that changes every 60 seconds. At login, authorized users enter their password and the code displayed on their SecurID token card. While a password may be compromised, the constantly changing access code, which requires the token card during system use, bars unauthorized users from entering the network.

Using the SecurID token card

Each SecurID token card is programmed with an algorithm that ensures every code displayed is valid only for that user at that particular time. The token card has a display that authorizes the individual user access to the computer. Through this authentication system, the user's identity is verified when the correct password and current code are entered from the user's token.

Personal identification number (PIN)

The user's password is called a personal identification number, or PIN. The user enters the secret PIN from a console connection, followed by the current code displayed on the token card. Then the access control module must authenticate the token's unique code in combination with the user's secret PIN before access is granted.

Key Security Authentication Features of the Netopia R2020

As a remote device, the Netopia R2020 offers client/calling side security authentication. This feature allows the Netopia R2020 to call a server router and perform security card authentication. The router of the called server must have access to a server with ACE software loaded on it.

To perform security card authentication, each user must have a security authentication token card and a PIN. In addition, the user's identifying information must reside on the remote ACE servers for authentication negotiation to properly take place.

The Netopia R2020 supports the following user configurations for security authentication:

- Single user, calling a single destination (single session)
- Single user, calling multiple destinations (two simultaneous and separate sessions)
- Multiple users, calling a single destination (single session)
- Multiple users, calling multiple destinations (two simultaneous and separate sessions

Security authentication components

To properly identify and authenticate an authorized user, the following are required:

- A secret personal identification number (PIN) for each user.
- A security authentication token card.
- A Security Access Control Module (ACM).

Note: The Netopia R2020 currently only supports Ascend routers as ACMs.

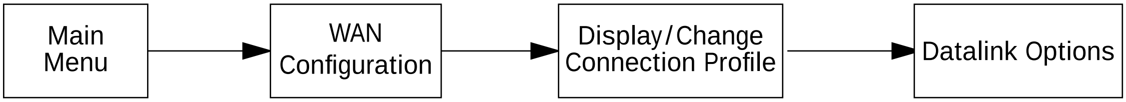
- An external Netopia R2020 calling into a designated server. For example, a telecommuter dialing into a remote site from a Netopia R2020 interested in accessing personal email or file sharing services.

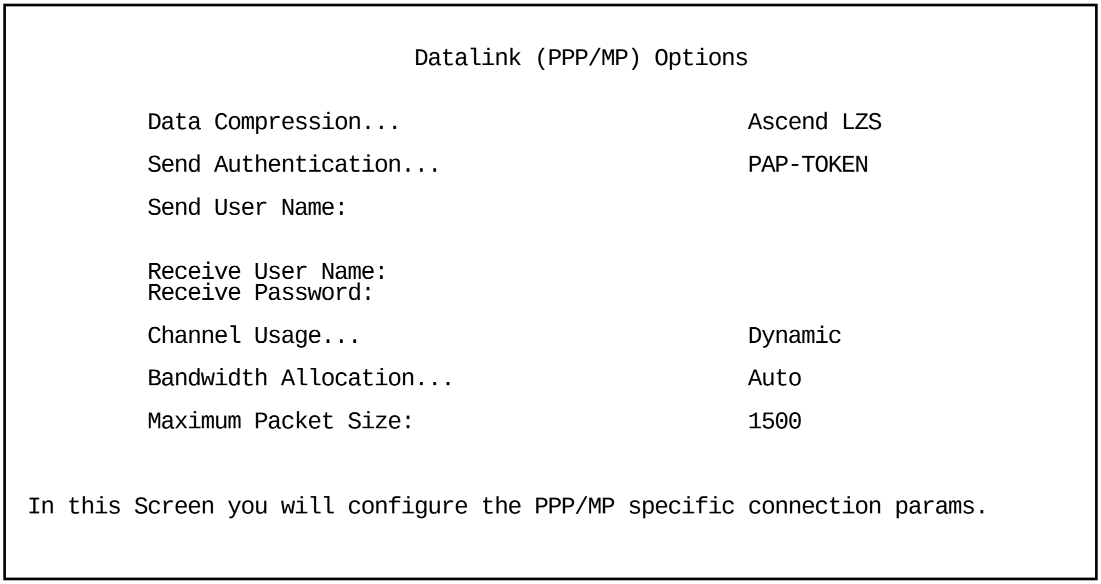
Note: The Netopia R2020 does not include a security authentication token card.

Configuring for security authentication

To configure the Netopia R2020 to support security authentication, select an authentication method and set up a designated connection profile from the System Configuration screen or your first connection profile from Easy Setup.

1. From the WAN Configuration menu, select Display/Change Connection Profile. From the pop-up menu that appears, select a Connection Profile. In the Connection Profile screen select **Datalink Options**.





```
                         Datalink (PPP/MP) Options

          Data Compression...                          Ascend LZS
          Send Authentication...                       PAP-TOKEN
          Send User Name:

          Receive User Name:
          Receive Password:

          Channel Usage...                             Dynamic
          Bandwidth Allocation...                      Auto
          Maximum Packet Size:                         1500


 In this Screen you will configure the PPP/MP specific connection params.
```

2. Select Send Authentication and press Return. From the pop-up menu, highlight **PAP-TOKEN** or **CACHE-TOKEN**. Your network administrator or the remote network administrator will tell you which method to select.

   If you select PAP-TOKEN, select **Send User Name** and enter a name for your Netopia R2020. You will not need to enter a Send Password for PAP-TOKEN. Press Return.

   If you select CACHE-TOKEN, select **Send User Name** and enter a name for your Netopia R2020. Then, select **Send Password** and enter a secret name or number. Press Return.

3. Set up a connection profile to use with your authentication method. For information on setting up a connection profile, see Chapter 6, “Easy Setup.”

Note: If you are setting up your first connection profile, you can also enter your authentication information in the Easy Setup Connection Profile screen.

Connecting using security authentication

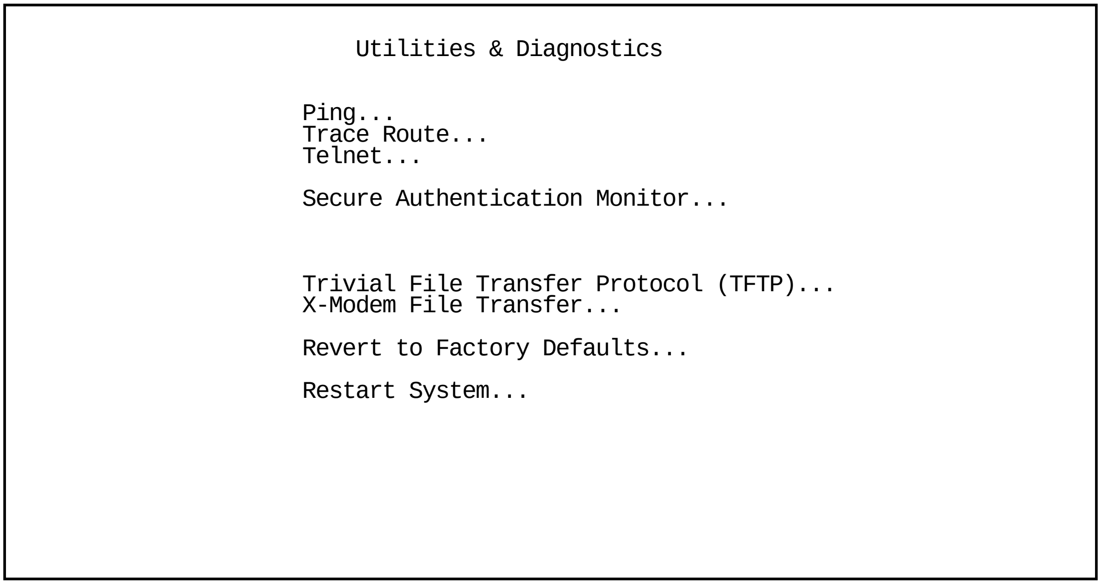
You can initiate a connection call using security authentication in either of two ways:

- establish a dial-on-demand (DOD) connection, or
- establish a manual connection.

Establishing a dial-on-demand (DOD) connection call

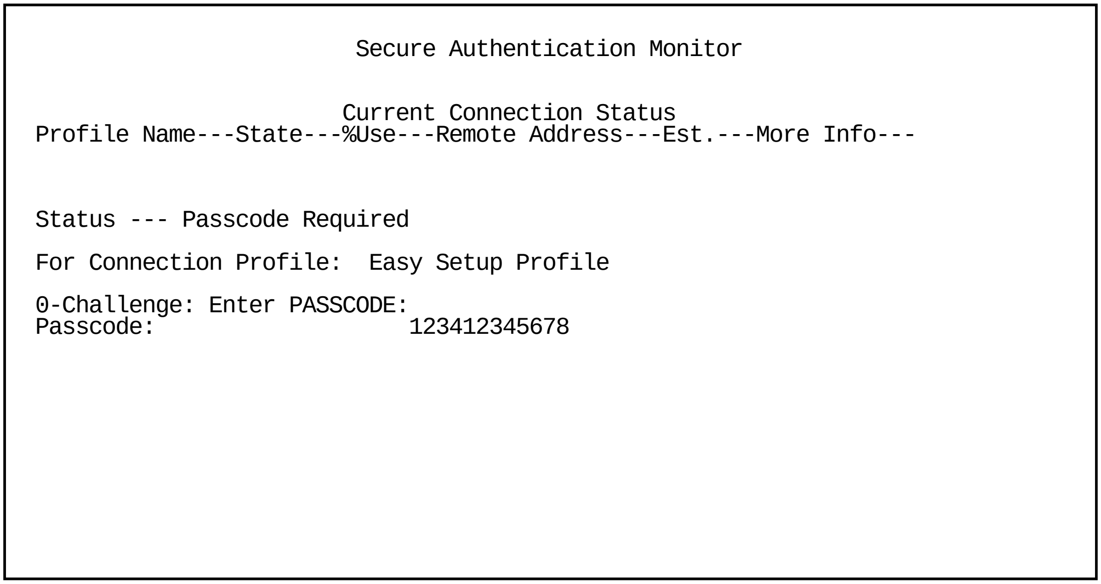
To establish a connection call using DOD, select Utilities & Diagnostics from the Main Menu and press Return.

Note: The Secure Authentication Monitor field will remain hidden if PAP-TOKEN or CACHE-TOKEN is not the selected authentication method in the connection profile.



```
                          Utilities & Diagnostics

                      Ping...
                      Trace Route...
                      Telnet...

                      Secure Authentication Monitor...


                      Trivial File Transfer Protocol (TFTP)...
                      X-Modem File Transfer...

                      Revert to Factory Defaults...

                      Restart System...
```

1. Select **Secure Authentication Monitor** and press Return. The Secure Authentication Monitor screen appears.
2. Wait for the call to initiate.



```
                          Secure Authentication Monitor


                         Current Connection Status
  Profile Name---State---%Use---Remote Address---Est.---More Info---



  Status --- Passcode Required

  For Connection Profile:  Easy Setup Profile

  0-Challenge: Enter PASSCODE:
  Passcode:                   123412345678
```

3. From the fields that appear, select **Enter PASSCODE** and press Return. Enter your PIN and the code displayed on your security authentication token card LED.
4. Once the call is established, and you enter your passcode as prompted, PPP negotiation will continue. If the call is specified for PAP-TOKEN, and the session involves more than one connection, you will be prompted for each connection being brought up.

Note: When using CACHE-TOKEN, your passcode is valid for a time interval determined by the network administrator. When this time interval expires, you must provide a new passcode for the call negotiation.

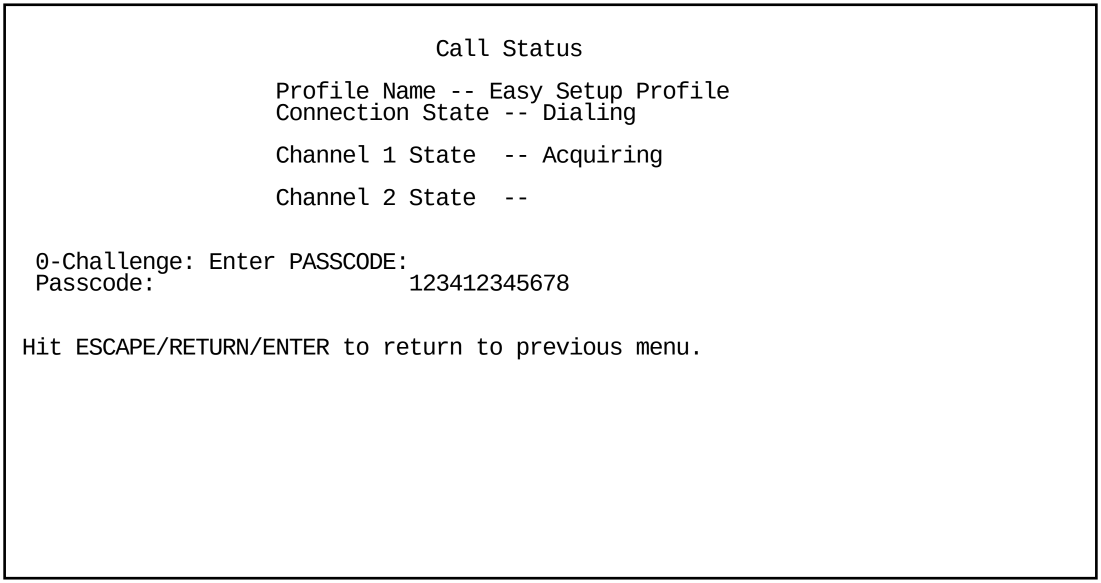
When using PAP-TOKEN, your passcode is valid for one call negotiation. For a second call negotiation, you must enter the next passcode provided by the security authentication token card every 60 seconds.

You will be able to access information at the remote site that you are connecting to once authentication is successfully completed.

Establishing a manual connection call

To establish a Manual connection call, select WAN Configuration from the Main Menu and press Return.

1. Select **Establish WAN Connection** from the WAN Configuration screen and press Return. The Establish WAN Connection screen displays a table of all of the connection profiles you have defined. Highlight the connection profile you wish to manually call. Press Return to initiate the call.



```
                              Call Status

                    Profile Name -- Easy Setup Profile
                    Connection State -- Dialing

                    Channel 1 State  -- Acquiring

                    Channel 2 State  --


  0-Challenge: Enter PASSCODE:
  Passcode:                   123412345678


 Hit ESCAPE/RETURN/ENTER to return to previous menu.
```

2. From the fields that appear, select **Enter PASSCODE** and press Return. Enter your PIN and the code displayed on your security authentication token card LED screen.
3. Once the call is established, and you enter your passcode as prompted, PPP negotiation will continue. If the call is specified for PAP-TOKEN, and the session involves more than one connection, you will be prompted for each channel being brought up.

Note: When using CACHE-TOKEN, your passcode is valid for a time interval determined by the network administrator. When this time interval expires, you must provide a new passcode for the call negotiation.

When using PAP-TOKEN for a dial-up call, your passcode is valid for one call negotiation. For a second call negotiation, you must enter the next passcode provided by the security authentication token card every 60 seconds.

You will be able to access information at the remote site that you are connecting to once authentication is successfully completed.

Chapter 15

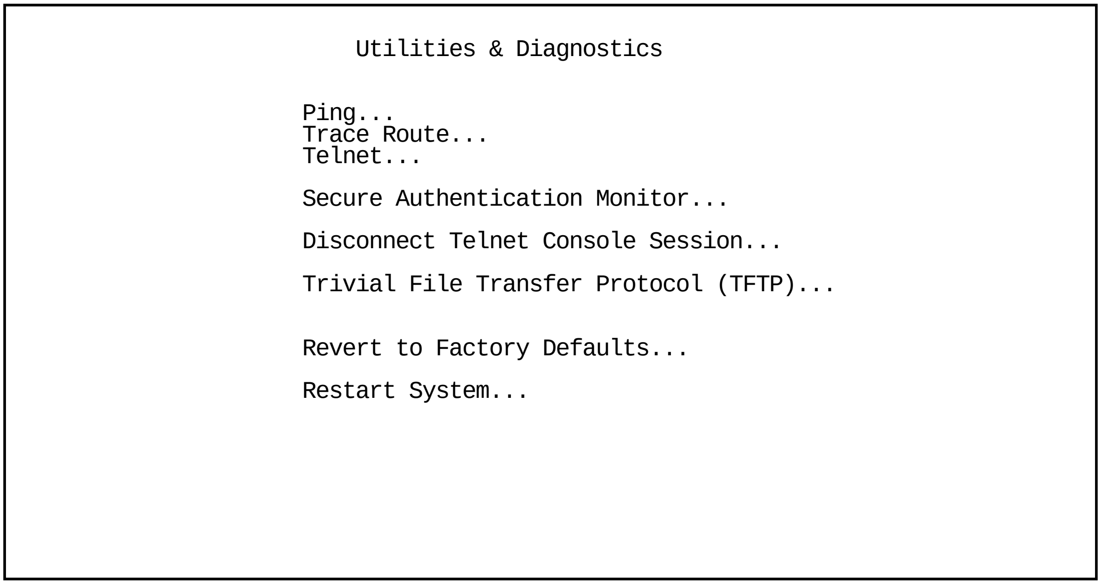
Utilities and Diagnostics

A number of utilities and tests are available for system diagnostic and control purposes:

- "Ping" on page 15-2
- "Trace Route" on page 15-5
- "Telnet client" on page 15-6
- "Secure Authentication Monitor" on page 15-6
- "Disconnect Telnet Console Session" on page 15-7
- "Transferring configuration and firmware files with TFTP" on page 15-7
- "Transferring configuration and firmware files with XMODEM" on page 15-10
- "Factory defaults" on page 15-7
- "Restarting the system" on page 15-13

Note: These utilities and tests are accessible only through the console-based management screens. See Chapter 5, "Console-based Management," for information on accessing the console-based management screens.

You access the **Utilities & Diagnostics** screens from the **Main Menu**.



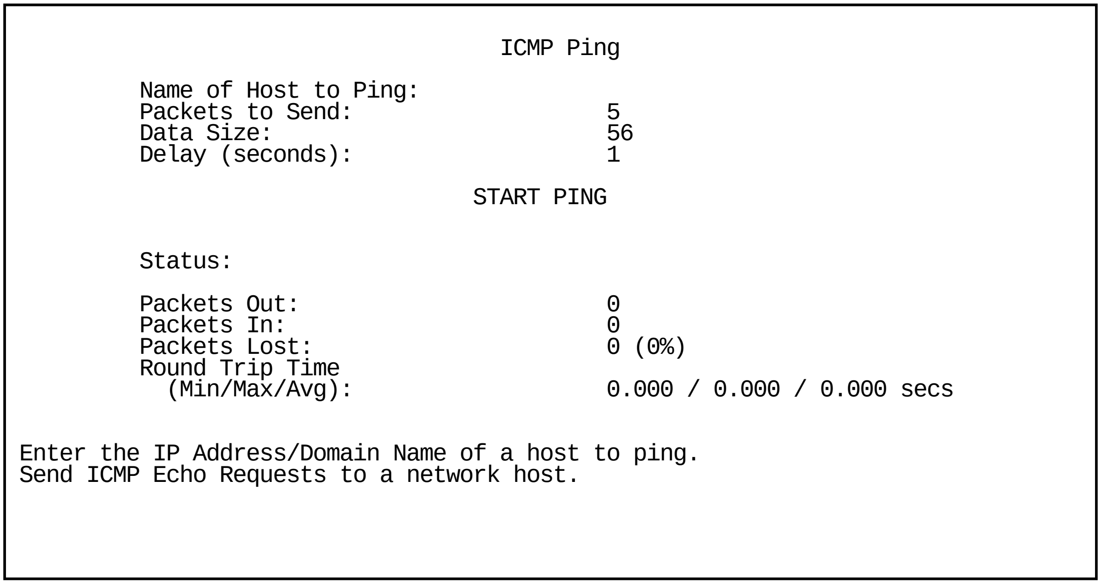
```
              Utilities & Diagnostics

          Ping...
          Trace Route...
          Telnet...

          Secure Authentication Monitor...

          Disconnect Telnet Console Session...

          Trivial File Transfer Protocol (TFTP)...


          Revert to Factory Defaults...

          Restart System...
```

Ping

The Netopia R2020 includes a standard Ping test utility. A Ping test generates IP packets destined for a particular (Ping-capable) IP host. Each time the target host receives a Ping packet, it returns a packet to the original sender.

Ping allows you to see whether a particular IP destination is reachable from the Netopia R2020. You can also ascertain the quality and reliability of the connection to the desired destination by studying the Ping test's statistics.

To use the Ping utility, select **Ping** in the Statistics, Utilities, Tests screen and press Return to go to the Ping screen.



```
                                ICMP Ping

         Name of Host to Ping:
         Packets to Send:                   5
         Data Size:                         56
         Delay (seconds):                   1

                              START PING


         Status:

         Packets Out:                       0
         Packets In:                        0
         Packets Lost:                      0 (0%)
         Round Trip Time
           (Min/Max/Avg):                   0.000 / 0.000 / 0.000 secs


Enter the IP Address/Domain Name of a host to ping.
Send ICMP Echo Requests to a network host.
```

To configure and initiate a Ping test, follow these steps:

1. Select **Name of Host to Ping** and enter the destination domain name or IP address.
2. Select **Packets to Send** to change the default setting. This is the total number of packets to be sent during the Ping test. The default setting is adequate in most cases, but you may change it to any value from 1 to 4,294,967,295.
3. Select **Data Size** to change the default setting. This is the size, in bytes, of each Ping packet sent. The default setting is adequate in most cases, but you may change it to any value from 0 (only header data) to 1664.
4. Select **Delay (seconds)** to change the default setting. The delay, in seconds, determines the time between Ping packets sent. The default setting is adequate in most cases, but you may change it to any value from 0 to 4,294,967. A delay of 0 seconds forces packets to be sent immediately one after another.
5. Select **START PING** and press Return to begin the Ping test. While the test is running, the **START PING** item becomes **STOP PING**. To manually stop the Ping test, select **STOP PING** and press Return or the Escape key.

While the Ping test is running, and when it is over, a status field and a number of statistical items are active on the screen. These are described below.

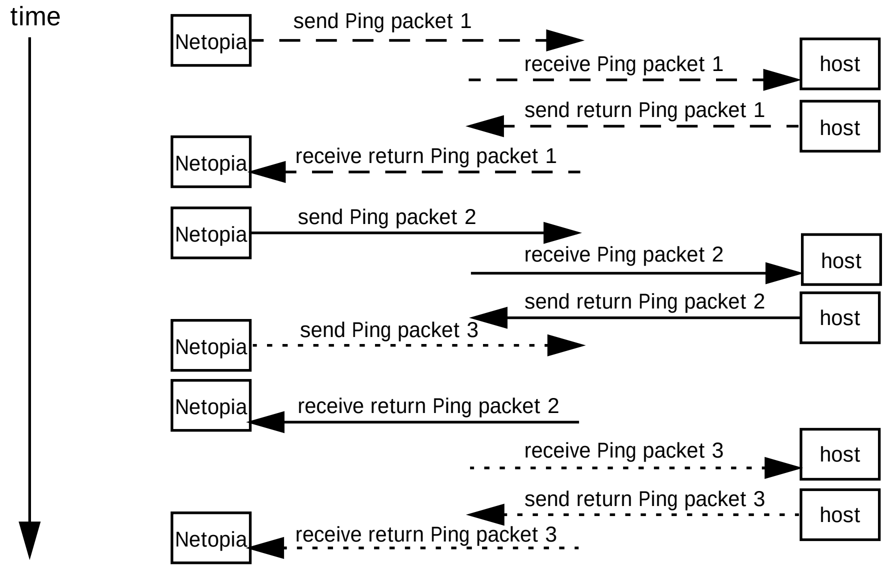
Status: The current status of the Ping test. This item can display the following messages:

Message	Description
Resolving host name	Finding the IP address for the domain name-style address
Can’t resolve host name	IP address can’t be found for the domain name-style name
Pinging	Ping test is in progress
Complete	Ping test was completed
Cancelled by user	Ping test was cancelled manually
Destination unreachable from w.x.y.z	Ping test was able to reach the router with IP address w.x.y.z, which reported that the test could not reach the final destination
Couldn’t allocate packet buffer	Couldn’t proceed with Ping test; try again or reset system
Couldn’t open ICMP port	Couldn’t proceed with Ping test; try again or reset system

Packets Out: The number of packets sent by the Ping test.

Packets In: The number of return packets received from the target host. To be considered “on time,” return packets are expected back before the next packet in the sequence of Ping packets is sent. A count of the number of late packets appears in parentheses to the right of the **Packets In** count.

In the example below, a Netopia R2020 is sending Ping packets to another host, which responds with return Ping packets. Note that the second return Ping packet is considered to be late because it is not received by the Netopia R2020 before the third Ping packet is sent. The first and third return Ping packets are on time.



Packets Lost: The number of packets unaccounted for, shown in total and as a percentage of total packets sent. This statistic may be updated during the Ping test, and may not be accurate until after the test is over. However, if an escalating one-to-one correspondence is seen between **Packets Out** and **Packets Lost**, and **Packets In** is noticeably lagging behind **Packets Out**, the destination is probably unreachable. In this case, use **STOP PING**.

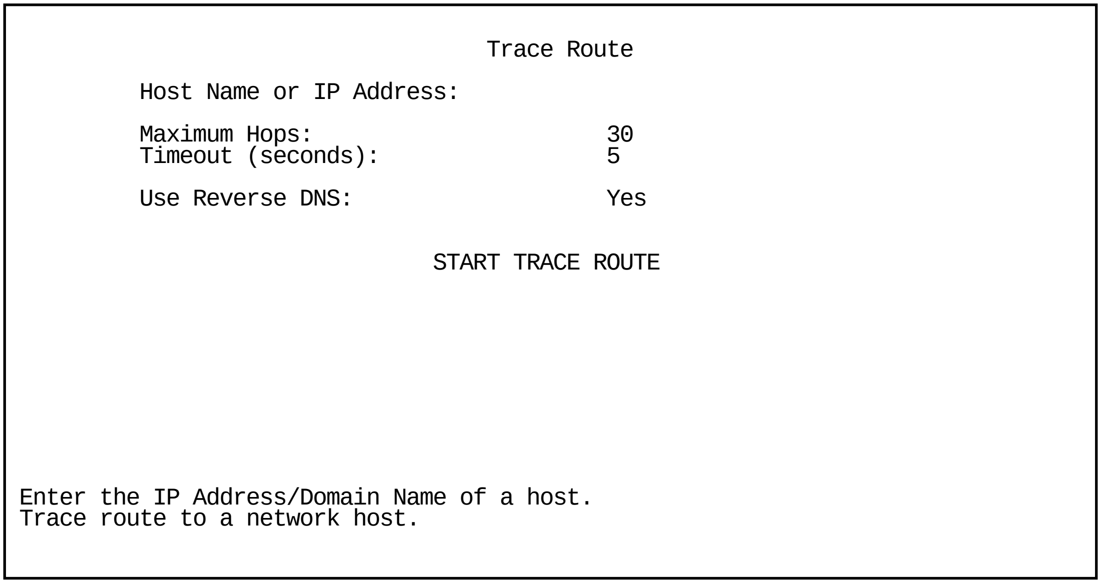
Round Trip Time (Min / Max / Avg): Statistics showing the minimum, maximum, and average number of seconds elapsing between the time each Ping packet was sent and the time its corresponding return Ping packet was received.

The time-to-live (TTL) value for each Ping packet sent by the Netopia R2020 is 255, the maximum allowed. The TTL value defines the number of IP routers that the packet can traverse. Ping packets that reach their TTL value are dropped, and a “destination unreachable” notification is returned to the sender (see the table above). This ensures that no infinite routing loops occur. The TTL value can be set and retrieved using the SNMP MIB-II ip group’s ipDefaultTTL object.

Trace Route

You can count the number of routers between your Netopia Router and a given destination with the Trace Route utility.

Select **Trace Route** in the Statistics & Diagnostics screen and press Return to go to the Trace Route screen.



```
                              Trace Route

         Host Name or IP Address:

         Maximum Hops:                      30
         Timeout (seconds):                 5

         Use Reverse DNS:                   Yes


                           START TRACE ROUTE








Enter the IP Address/Domain Name of a host.
Trace route to a network host.
```

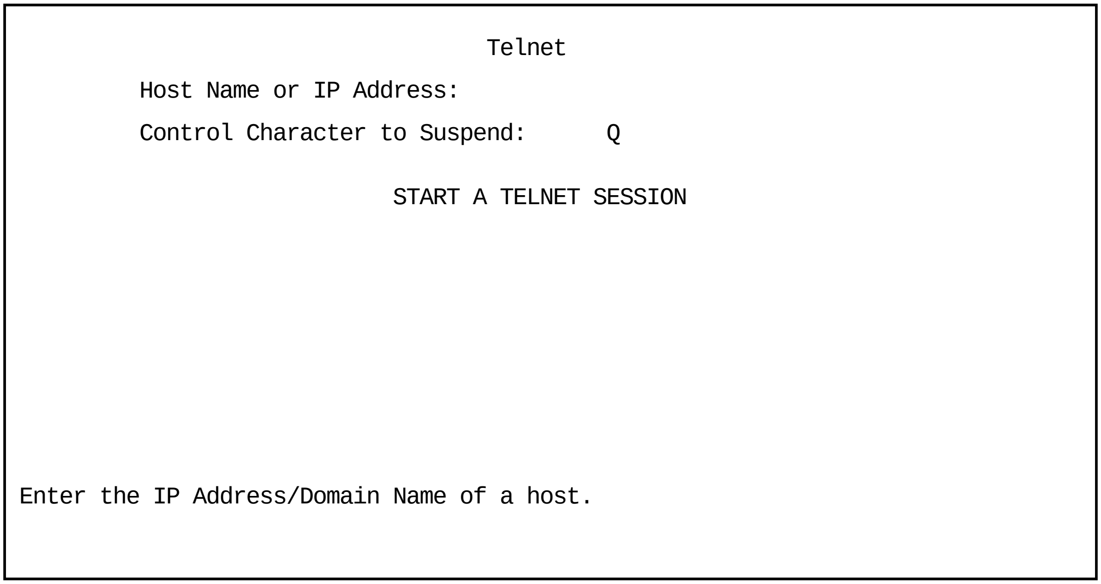
To trace a route, follow these steps:

1. Select **Host Name or IP Address** and enter the name or address of the destination you want to trace.
2. Select **Maximum hops (1..64)** to set the maximum number of routers to count between the Netopia Router and the destination router, up to the maximum of 64. The default is 30 hops.
3. Select **Timeout per probe (1..10 sec)** to set when the trace will timeout for each hop, up to 10 seconds. The default is 3 seconds.
4. Select **Use Reverse DNS** to learn the names of the routers between the Netopia Router and the destination router. The default is Yes.
5. Select **START TRACE ROUTE** and press Return. The screen will be replaced by a scrolling screen, listing the destination, the number of hops, the IP addresses of each hop, and the DNS names, if selected.
6. Cancel the trace by pressing Escape. Return to the Trace Route screen by pressing Escape twice.

Telnet client

The Telnet client mode replaces the normal menu mode. Telnet sessions can be cascaded, that is, you can initiate a Telnet client session when using a Telnet console session. To activate the Telnet client, select **Telnet** from the Utilities & Diagnostics menu.

The Telnet client screen appears.



```
                                 Telnet

          Host Name or IP Address:

          Control Character to Suspend:      Q

                          START A TELNET SESSION










Enter the IP Address/Domain Name of a host.
```

- Enter the host name or the IP address in dotted decimal format of the machine you want to telnet into and press Return.
- Either accept the default control character "Q" used to suspend the Telnet session, or type a different one.
- **START A TELNET SESSION** becomes highlighted.
- Press Return and the Telnet session will be initiated.
- To suspend the session, press Control-Q, or whatever other control character you specified.

  Two new options will appear in the Telnet screen (not shown):

  Resume Suspended Session – select this one if you want to go back to your Telnet session

  Terminate Suspended Session – select this one if you want to end the session

Secure Authentication Monitor

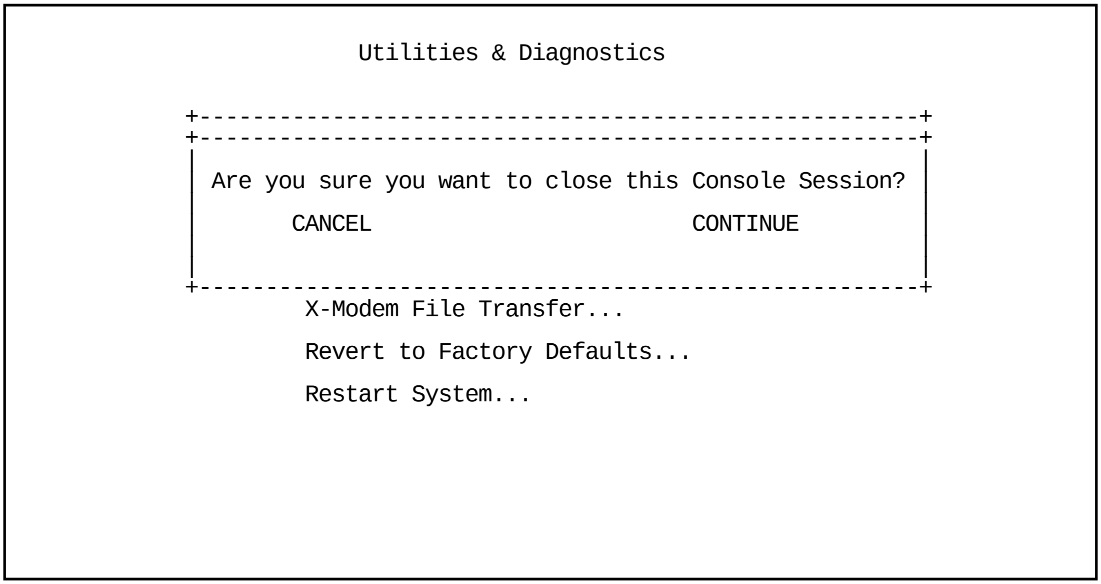
Note: The Secure Authentication Monitor field will remain hidden if PAP-TOKEN or CACHE-TOKEN is not the selected authentication method in the Connection Profile.

You use the Secure Authentication Monitor screen when placing one type of SecurID connection call. See "Connecting using security authentication" on page 14-38 for details.

Disconnect Telnet Console Session

If you want to close your Telnet Console session, select **Disconnect Telnet Console Session** and press Return.

A dialog box appears asking you to cancel or continue your selection.



```
                          Utilities & Diagnostics

              +-------------------------------------------------------+
              +-------------------------------------------------------+
              |                                                       |
              | Are you sure you want to close this Console Session?  |
              |       CANCEL                        CONTINUE          |
              |                                                       |
              |                                                       |
              +-------------------------------------------------------+
                       X-Modem File Transfer...
                       Revert to Factory Defaults...
                       Restart System...
```

If you select **Continue**, you will immediately terminate your session.

Factory defaults

You can reset the Netopia R2020 to its factory default settings. Select the **Revert to Factory Defaults** item in the Statistics & Diagnostics screen and press Return. Select **CONTINUE** in the dialog box and press Return. The Netopia R2020 will reboot and its settings will return to the factory defaults, deleting your configurations.

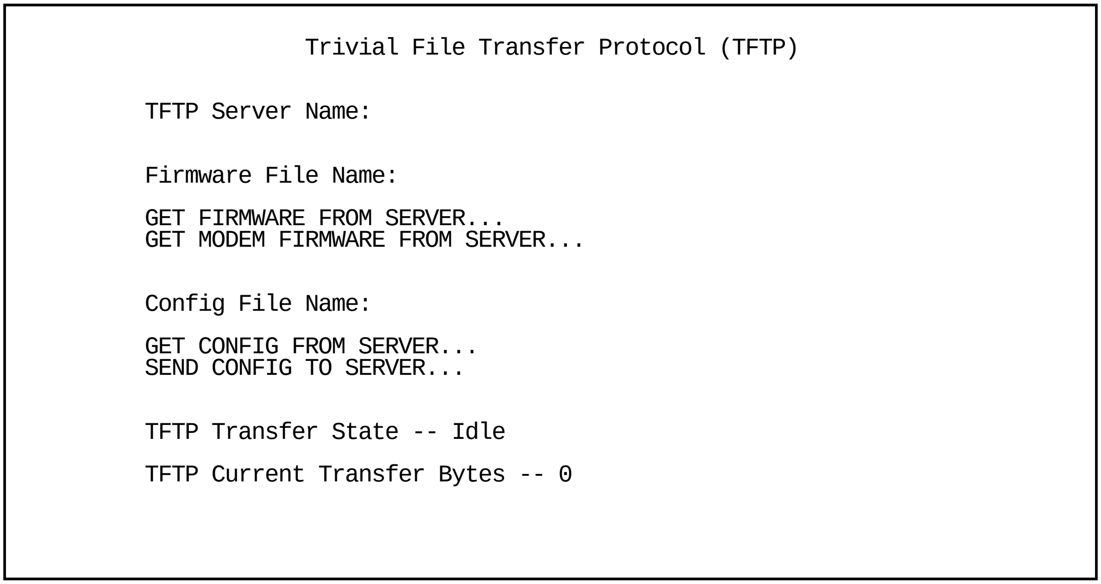
In an emergency, you can also use the Reset Switch to return the router to its factory default settings. Call Netopia Tech Support for instructions on using the Reset Switch.

Note: Reset to factory defaults with caution. You will need to reconfigure all your settings in the router.

Transferring configuration and firmware files with TFTP

Trivial File Transfer Protocol (TFTP) is a method of transferring data over an IP network. TFTP is a client-server application, with the Router as the client. To use the Router as a TFTP client, a TFTP server must be available. Netopia, Inc. has a public access TFTP server on the Internet where you can obtain the latest firmware versions.

To use TFTP, select **Trivial File Transfer Protocol (TFTP)** in the Statistics & Diagnostics screen and press Return to go to the Trivial File Transfer Protocol (TFTP) screen.



```
                     Trivial File Transfer Protocol (TFTP)

          TFTP Server Name:


          Firmware File Name:

          GET FIRMWARE FROM SERVER...
          GET MODEM FIRMWARE FROM SERVER...


          Config File Name:

          GET CONFIG FROM SERVER...
          SEND CONFIG TO SERVER...


          TFTP Transfer State -- Idle

          TFTP Current Transfer Bytes -- 0
```

The sections below describe how to update the Router’s firmware and how to download and upload configuration files.

Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization’s network administrator.

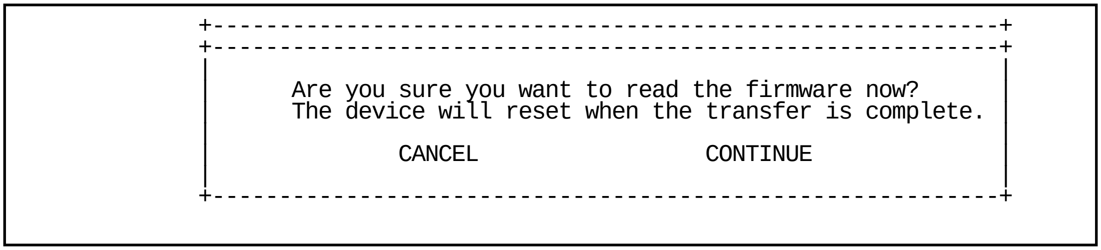
There are two types of firmware in the Netopia R2020 Dual Analog Router: router firmware and modem firmware. The router firmware governs how the router communicates with your network and the modems; the modem firmware governs how the modems communicate with the remote site. Modem firmware, for example to support the ITU V.90 standard, is included on your Netopia CD for XMODEM transfer and later updates will be available on the Netopia website. Router firmware updates are also periodically posted on the Netopia website.

To update either the Router’s or the internal modems’ firmware, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
- Select **Firmware File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file

name (for example, bigroot/config/myfile).

- Select **Send Firmware to Netopia from TFTP Server** and press Return. You will see the following dialog box:



```
+-------------------------------------------------------------+
+-------------------------------------------------------------+
|                                                             |
|      Are you sure you want to read the firmware now?        |
|      The device will reset when the transfer is complete.   |
|                                                             |
|              CANCEL                 CONTINUE                |
|                                                             |
+-------------------------------------------------------------+
```

- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

- Be sure the firmware update you load onto your router is the correct version for your particular model. Some models do not support all firmware versions. Loading an incorrect firmware version can permanently damage the unit.
- Do not manually power down or reset the Netopia R2020 while it is automatically resetting or it could be damaged.
- If you choose to download the firmware, the **TFTP Transfer State** item will change from **Idle** to **Reading Firmware**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Downloading configuration files

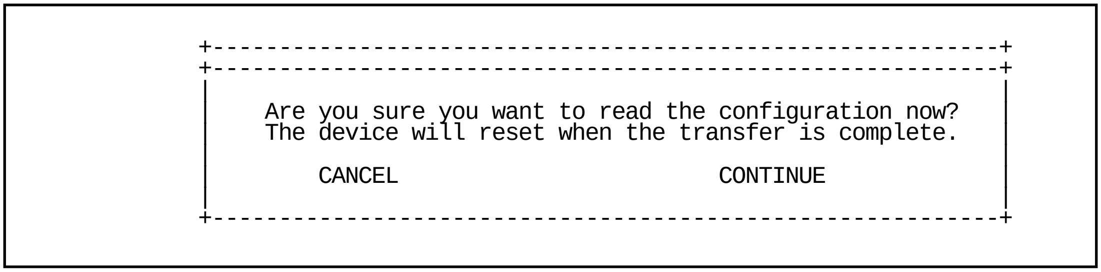
The Router can be configured by downloading a configuration file using TFTP. Once downloaded, the file reconfigures all of the Router’s parameters as if someone had manually done so through the console port.

To download a configuration file, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
- Select **Config File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for

example, bigroot/config/myfile).

- Select **Read Config Now** and press Return. You will see the following dialog box:



```
+-----------------------------------------------------------+
+-----------------------------------------------------------+
|                                                           |
|    Are you sure you want to read the configuration now?   |
|    The device will reset when the transfer is complete.   |
|                                                           |
|        CANCEL                        CONTINUE             |
|                                                           |
+-----------------------------------------------------------+
```

- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new configuration into effect.
- If you choose to download the configuration file, the **TFTP Transfer State** item will change from **Idle** to **Reading Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Uploading configuration files

Using TFTP, you can send a file containing a snapshot of the Router’s current configuration to a TFTP server. The file can then be downloaded by a different Netopia R2020 unit to configure its parameters (see “Downloading configuration files” on page 15-9). This is useful for configuring a number of Routers with identical parameters, or just for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia R2020 unit by Netopia or your network administrator.

To upload a configuration file, follow these steps:

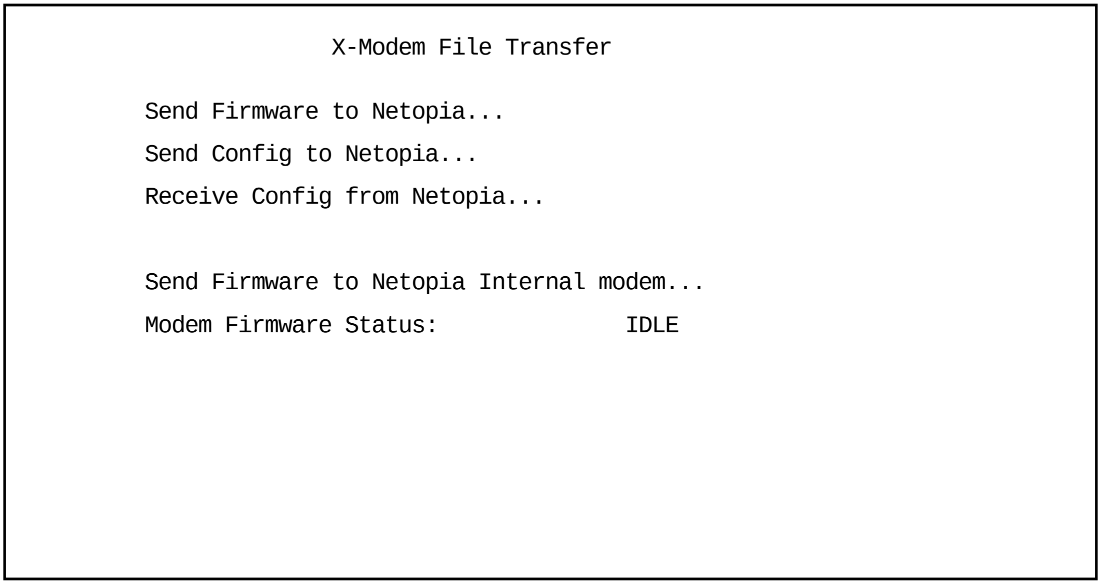
1. Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
2. Select **Config File Name** and enter a name for the file you will upload. The file will appear with the name you choose on the TFTP server. You may need to enter a file path along with the file name (for example, Mypc/Netopia/myfile).
3. Select **Write Config Now** and press Return. Netopia will begin to transfer the file.
4. The **TFTP Transfer State** item will change from **Idle** to **Writing Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Transferring configuration and firmware files with XMODEM

You can transfer configuration and firmware files with XMODEM through the Netopia R2020’s console port. Be sure your terminal emulation program supports XMODEM file transfers.

To go to the **X-Modem File Transfer** screen, select it in the Utilities & Diagnostics screen.

Note: The X-Modem File Transfer screen is only available if you are connected via the Console port.



```
                        X-Modem File Transfer

          Send Firmware to Netopia...

          Send Config to Netopia...

          Receive Config from Netopia...


          Send Firmware to Netopia Internal modem...

          Modem Firmware Status:              IDLE
```

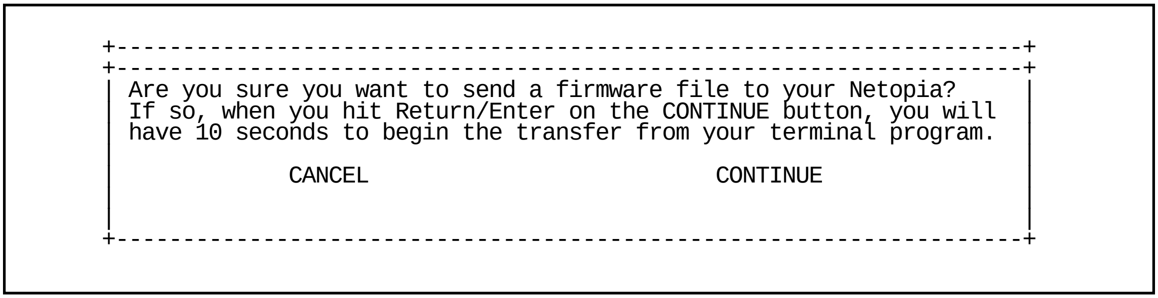
Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization’s network administration.

The procedure below applies whether you are using the console or the built-in modems.

Follow these steps to update the Netopia R2020’s firmware:

1. Make sure you have the firmware file on disk and know the path to its location.
2. Select **Send Firmware to Netopia** (or **Send Firmware to Netopia WAN module**) and press Return. The following dialog box appears:



```
+---------------------------------------------------------------------+
+---------------------------------------------------------------------+
| Are you sure you want to send a firmware file to your Netopia?      |
| If so, when you hit Return/Enter on the CONTINUE button, you will   |
| have 10 seconds to begin the transfer from your terminal program.   |
|                                                                     |
|             CANCEL                          CONTINUE                |
|                                                                     |
|                                                                     |
+---------------------------------------------------------------------+
```

3. Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

   If you choose **CONTINUE**, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the firmware file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer’s failure. You can then try again.

The system will reset at the end of a successful file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

Do not manually power down or reset the Netopia R2020 while it is automatically resetting or it could be damaged.

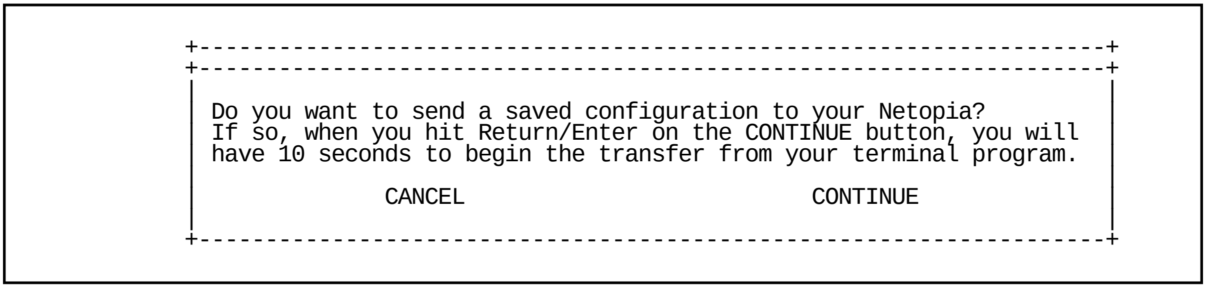
Downloading configuration files

The Netopia R2020 can be configured by downloading a configuration file. The downloaded file reconfigures all of the Router's parameters.

Configuration files are available from a site maintained by your organization's network administrator or from your local site (see "Uploading configuration files," below).

Follow these steps to download a configuration file:

1. Make sure you have the configuration file on disk and know the path to its location.
2. Select **Send Config to Netopia** and press Return. The following dialog box appears:



```
+----------------------------------------------------------------------+
+----------------------------------------------------------------------+
|                                                                      |
|  Do you want to send a saved configuration to your Netopia?          |
|  If so, when you hit Return/Enter on the CONTINUE button, you will   |
|  have 10 seconds to begin the transfer from your terminal program.   |
|                                                                      |
|                CANCEL                          CONTINUE              |
|                                                                      |
+----------------------------------------------------------------------+
```

3. Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

   If you choose **CONTINUE**, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

   The system will reset at the end of a successful file transfer to put the new configuration into effect.

Uploading configuration files

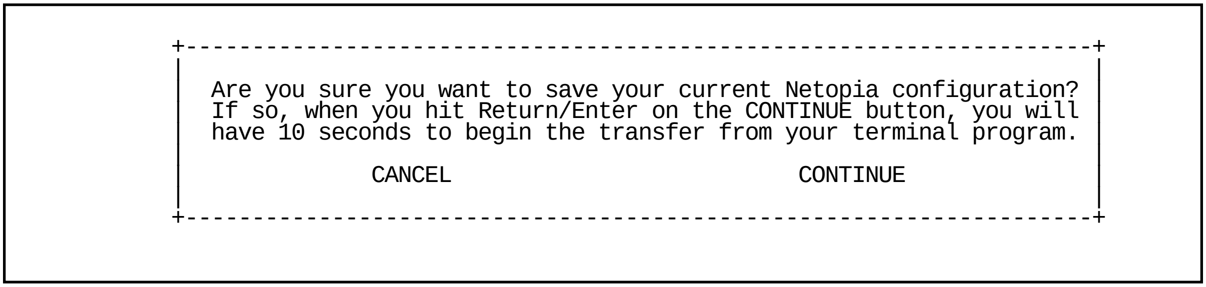
A file containing a snapshot of the Netopia R2020's current configuration can be uploaded from the Router to disk. The file can then be downloaded by a different Netopia R2020 to configure its parameters (see "Downloading configuration files" on page 15-12). This is useful for configuring a number of Routers with identical parameters, or for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia R2020 by Netopia or your network administrator.

The procedure below applies whether you are using the console or the built-in modems.

To upload a configuration file:

1. Decide on a name for the file and a path for saving it.
2. Select **Receive Config from Netopia** and press Return. The following dialog box appears:



```
+--------------------------------------------------------------------+
|                                                                    |
|  Are you sure you want to save your current Netopia configuration? |
|  If so, when you hit Return/Enter on the CONTINUE button, you will |
|  have 10 seconds to begin the transfer from your terminal program. |
|                                                                    |
|              CANCEL                          CONTINUE              |
|                                                                    |
+--------------------------------------------------------------------+
```

3. Select **CANCEL** to exit without uploading the file, or select **CONTINUE** to upload the file.

   If you choose **CONTINUE**, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

Restarting the system

You can restart the system by selecting the **Restart System** item in the Utilities & Diagnostics screen.

You must restart the system whenever you reconfigure the Netopia R2020 and want the new parameter values to take effect. Under certain circumstances, restarting the system may also clear up system or network malfunctions. Some configuration processes automatically restart the system to apply the changes you have made.

Part III: Appendixes

Appendix A

Troubleshooting

This appendix is intended to help you troubleshoot problems you may encounter while setting up and using the Netopia R2020. It also includes information on how to contact Netopia Technical Support.

Important information on these problems may be found in the event histories kept by the Netopia R2020. These event histories can be accessed in the Statistics, Utilities, Tests screen.

This section covers the following topics:

- "Configuration problems" on page A-1
- "Power outages" on page A-3
- "Technical support" on page A-3

Configuration problems

If you encounter problems during your initial configuration process, review the following suggestions before calling for technical support. There are four zones to consider when troubleshooting initial configuration:

1. the computer's connection to the router;
2. the router's connection to the telecommunication line(s);
3. the telecommunication line's connection to your ISP, and
4. the ISP's connection to the Internet.

If the connection from the computer to the router was not successful, check the following:

- The Netopia R2020 is turned on.
- An Ethernet cable connects your PC's Ethernet card or built-in Ethernet port to the Netopia R2020.
- The SmartStart application is running and able to access the Netopia R2020.
- Telnet is available on your PC or Macintosh. (On a PC, it must be specified in your system path. You can usually find the application as "c:\windowselnet.exe".)
- Your PC or Macintosh is properly configured for TCP/IP.
- Your PC or Macintosh has an IP address.
- Your PC or Macintosh has a subnet mask that matches or is compatible with the Netopia R2020's subnet mask.
- If you are entering a new IP address via SmartStart be sure the correct serial number was entered.

Note: If you are attempting to modify the IP address or subnet mask from a previous, successful configuration attempt, you will need to clear the IP address or reset your Netopia R2020 to the factory default before reinitiating the configuration process. For further information on resetting your Netopia R2020 to factory default, see "Factory defaults" on page 15-7.

SmartStart Troubleshooting

The Status field of the SmartStart application will display information and indicate problems as they are detected.

Console connection problems

Can't see the configuration screens (nothing appears)

- Check the cable connection from the Netopia R2020's console port to the computer being used as a console.
- Check that the terminal emulation software is accessing the correct port on the computer that's being used as a console.
- Try pressing Ctrl-L or Return or the ▲ up or down▼ key several times to refresh the terminal screen.
- Check that flow control on serial connections is turned off.

Junk characters appear on the screen

- Check that the terminal emulation software is configured correctly.
- Check the baud rate. The default values are 9600, N, 8, and 1.

Characters are missing from some of the configuration screens

- Try changing the Netopia R2020's default speed of 9600 bps and setting your terminal emulation software to match the new speed.

Network problems

This section contains tips on ways you can troubleshoot a networking problem.

Problems communicating with remote IP hosts

- Verify the accuracy of the default gateway's IP address (entered in the IP Setup or Easy Setup screen).
- Use the Netopia R2020's ping utility, in the Statistics, Tests, Utilities screen, and try to ping local and remote hosts. See "Ping" on page 15-2 for instructions on how to use the ping utility. If you can successfully ping hosts using their IP addresses but not their domain names (198.34.7.1 but not garcia.netopia.com, for example), verify that the DNS server's IP address is correct and that it is reachable from the Netopia R2020 (use ping).
- If you are using filters, check that your filter sets are not blocking the type of connections you are trying to make.

Local routing problems

- Observe the Ethernet LEDs to see if data traffic flow appears to be normal.
- Check the WAN Statistics and LAN Statistics screens to see more specific information on data traffic flow and address serving.

Power outages

If you suspect that power was restored after a power outage, and the Netopia R2020 is connected to a remote site, you may need to switch the Netopia R2020 off and then back on again. After temporary power outages, a connection that still seems to be up may actually be disconnected. Rebooting the Router should reestablish the connection.

Technical support

Netopia, Inc. is committed to providing its customers with reliable products and documentation, backed by excellent technical support.

Before contacting Netopia

Look in this guide for a solution to your problem. You may find a solution in this troubleshooting appendix or in other sections. Check the index for a reference to the topic of concern. If you cannot find a solution, complete the environment profile below before contacting technical support.

Environment profile

- Locate the Netopia R2020's model number, product serial number, and firmware version. The serial number is on the bottom side of the Router, along with the model number. The firmware version appears in the Netopia R2020's Main Menu screen.

  Model number:

  Serial number:

  Firmware version:

- What kind of local network(s) do you have, with how many devices?

  Ethernet

  LocalTalk

  EtherTalk

  TCP/IP

  IPX

  Other:

How to reach us

We can help you with your problem more effectively if you have completed the environment profile in the previous section. If you contact us by telephone, please be ready to supply Netopia Technical Support with the information you used to configure the Netopia R2020. Also, please be at the site of the problem and prepared to reproduce it and to try some troubleshooting steps.

When you are prepared, contact Netopia Customer Service by e-mail, telephone, fax, or post:

Internet: techsports@netopia.com (for technical support)
info@netopia.com (for general information)

Phone: 1 800-782-6449
Fax: 1 510-814-5023

Netopia, Inc.
Customer Service
2470 Mariner Square Loop
Alameda, California 94501
USA

Netopia Bulletin Board Service: 1 510-865-1321

Online product information

Product information can be found in the following:

Netopia World Wide Web server via http://www.netopia.com
Internet via anonymous FTP to ftp.netopia.com/pub

FAX-Back

This service provides technical notes which answer the most commonly asked questions, and offer solutions for many common problems encountered with Netopia products.

FAX-Back: +1 510-814-5040

Appendix B

Setting Up Internet Services

This chapter describes how to obtain and set up Internet Services.

This section covers the following topics:

Note: Some companies act as their own ISP. For example, some organizations have branch offices that can use the Netopia R2020 to access the Internet via the main office in a point-to-point scenario. If you install the Netopia R2020 in this type of environment, refer to the following sections for specific information you must receive from the network administrator to configure the Netopia R2020 properly.

Finding an Internet service provider

During the setup session, the SmartStart setup application will provide you with a list of service providers who support the Netopia R2020 with Dual Analog. You can register with one of these ISPs as part of setting up your router.

If you have purchased your Netopia R2020 through a Netopia ISP partner, you may have received a customized configuration file from the ISP that will allow you to make an immediate connection when you run SmartStart.

Internet access is available from other Internet service providers. Typically, there are several ISPs in each area. To locate ISPs in your area, consult your telephone book, local computer magazines, the business section of a local newspaper, or the following URL on the Internet: ‘http://thelist.internet.com’. Also see Netopia’s home page at ‘http://www.netopia.com’ for a list of ISPs with special programs and promotions for Netopia customers.

If your area has more than one ISP, the following considerations may help you decide which ISP is best suited for your requirements.

Use an ISP that provides Internet access through a V.90 or K56flex line and supports dual analog LAN connections using Multilink PPP. If you would like to use an ISP that you already have a relationship with but is not familiar with the Netopia R2020 Dual Analog Router or using Multilink PPP with analog modems, call us at 1-800-NETOPIA. Our representative can call your ISP and introduce them to the product. As necessary, we can provide them with the technical background they need to support the product.

See “About 56K Line Access” on page G-1 for more information on 56K modem connections.

Unique requirements

Make sure the ISP can meet any unique requirements you may have. Potential requirements include:

- Dynamic or static IP addressing
- Class C IP address
- Custom domain name
- Multiple email addresses
- Web site hosting
- Call back for web site hosting at your site

Pricing and support

Compare pricing, service, and technical support service among various ISPs.

ISP’s Point of presence

Check with your ISP for the location of their nearest point of presence (POP) in reference to your site. In some instances, the ISP that you choose may not offer a POP in your local area. If that is the case, you may incur additional fees for long-distance calls.

Endorsements

Consider recommendations from colleagues and reviews in publications. Netopia lists Netopia Certified ISPs on our web site at ‘http://www.netopia.com’.

Deciding on an ISP account

Your ISP may offer various Internet access account plans. Typically, these plans vary by usage charges and the number of host IP addresses supplied. Evaluate your networking needs and discuss them with your ISP before deciding on a plan for your network.

The following checklist is a guide to ensure you obtain the Internet service you require.

Setting up a Netopia R2020 account

Check whether your ISP has the Netopia R2020 on a list of supported products that have been tested with a particular configuration. If the ISP does not have the Netopia R2020 on such a list, describe the Netopia R2020 in as much detail as needed, so your ISP account can be optimized. As appropriate, you may refer your ISP to Netopia’s web site for more information.

Obtaining an IP host address

Typically, each computer on the network that requires Internet access requires its own unique IP address. If some or all network computers require simultaneous Internet access, obtain a block of IP host addresses large enough for each computer to have its own address, plus one for the Netopia R2020.

Consider expected growth in your network when deciding on the number of addresses to obtain. Alternatively, you may use the Network Address Translation feature of SmartIP.

SmartIP™

The Netopia R2020 with Dual Analog supports the SmartIP™ feature which includes Network Address Translation.

Network Address Translation provides Internet access to the network connected to the Netopia R2020 using only a single IP address. These routers translate between the internal or local area network (LAN) addresses and a single external IP address and route accordingly.

For more information on Network Address Translation, see Chapter 10, “Multiple Network Address Translation and IP Setup.”

Obtaining information from the ISP

After your account is set up, the ISP should send you the IP parameter information that will help you to configure the Netopia R2020.

Local LAN IP address information to obtain (NAT enabled)

If you are using SmartIP (NAT), you should obtain the following:

- If you are dialing out to a remote site using Network Address Translation on your router, your provider will not define the IP address information on your local LAN. You can define this information based on parameters defined by another connection profile such as that to a corporate network, or an IP configuration that may already be in place for the existing network. Alternatively, you can use the default IP address range used by the router.
- Primary and Secondary Domain Name Server (DNS) IP Addresses
- Domain Name (usually the same as the ISP’s domain name unless you have registered for your own individual domain name)

Remote WAN IP address information to obtain

- Telephone number of the ISP’s local or nearby dial-up POP (point-of-presence).
- PPP authentication type for router at the ISP, such as PAP.
- Send and receive User Login name and Send and receive User Password if PAP or CHAP security authentication is used

Local LAN IP address information to obtain (NAT-disabled)

If you are not using SmartIP (NAT), you should obtain:

- The number of Ethernet IP host addresses available with your account and the first usable IP host address in the address block

- The Ethernet IP address for your Netopia R2020
- The Ethernet IP subnet mask address for your Netopia R2020
- The Default Gateway IP Address (same as Remote IP Address in most cases)
- Primary and Secondary Domain Name Server IP Addresses
- Domain Name (usually the same as the ISP’s domain name unless you have registered for your own individual domain name)

Note: If you are not using Network Address Translation, you will need to obtain all of the Local LAN IP address information from your ISP.

Remote WAN IP address information to obtain

- The telephone number of the ISP’s local or nearby dial-up POP (point-of-presence).
- Remote IP address of router at ISP or other remote site
- Remote IP subnet mask address of router at ISP or other remote site
- PPP authentication type for router at the ISP, such as PAP.
- Send User Login name and Send User Password if PAP or CHAP security authentication is used

Note: If you are not using Network Address Translation, you will need to obtain all of the Remote WAN IP address information from your ISP.

Appendix C

Understanding IP Addressing

This appendix is a brief general introduction to IP addressing. A basic understanding of IP will help you in configuring the Netopia R2020 and using some of its powerful features, such as static routes and packet filtering.

In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

This section covers the following topics:

What is IP?

All networks use protocols to establish common standards for communication. One widely used network protocol is the Internet Protocol, also known as IP. Like many other protocols, IP uses packets, or formatted chunks of data, to communicate.

Note: This guide uses the term "IP" in a very general and inclusive way, to identify all of the following:

- Networks that use the Internet Protocol, along with accompanying protocols such as TCP, UDP, and ICMP
- Packets that include an IP header within their structure
- Devices that send IP packets

About IP addressing

Every networking protocol uses some form of addressing in order to ensure that packets are delivered correctly. In IP, individual network devices that are initial sources and final destinations of packets are usually called hosts, instead of nodes, but the two terms are interchangeable. Each host on an IP network must have a unique IP address. An IP address, also called an Internet address, is a 32-bit number usually expressed as four decimal numbers separated by periods. Each decimal number in an IP address represents a 1-byte (8-bit) binary number. Thus, values for each of the four numbers range from 00000000 to 11111111 in binary notation, or from 0 to 255 in decimal notation. The expression 192.168.1.1 is a typical example of an IP address.

IP addresses indicate both the identity of the network and the identity of the individual host on the network. The number of bits used for the network number and the number of bits used for the host number can vary, as long as certain rules are followed. The local network manager assigns IP host numbers to individual machines.

IP addresses are maintained and assigned by the InterNIC, a quasi-governmental organization now increasingly under the auspices of private industry.

Note: It's very common for an organization to obtain an IP address from a third party, usually an Internet service provider (ISP). ISPs usually issue an IP address when they are contracted to provide Internet access services.

The InterNIC (the NIC stands for Network Information Center) divides IP addresses into several classes. Classes A, B, and C are assigned to organizations who request addresses. In Class A networks, the first byte of an IP address is reserved for the network portion of the address. Class B networks reserve the first two bytes of an IP address for the network address. Class C networks reserve the first three bytes of an IP address for the network address. In all cases, a network manager can decide to use subnetting to assign even more bits to the network portion of the IP address, but never less than the class requires. The following section gives more information on subnetting.

Class A networks have a small number of possible network numbers, but a large number of possible host numbers. Conversely, Class C networks have a small number of possible host numbers, but a large number of possible network numbers. Thus, the InterNIC assigns Class A addresses to large organizations that have very large numbers of IP hosts, while smaller organizations, with fewer hosts, get Class B or Class C addresses. You can tell the various classes apart by the value of the first (or high-order) byte. Class A networks use values from 1 to 127, Class B networks use values from 128 to 191, and Class C networks use values from 192 to 223. The following table summarizes some of the differences between Class A, B, and C networks.

Class	First byte	Number of networks possible per class	Number of hosts possible per network	Format of address (without subnetting)	Example
A	1-127	127	16,777,214	net.host.host.host	97.3.14.250
B	128-191	16,384	65,534	net.net.host.host	140.100.10.11
C	192-223	2,097,152	254	net.net.net.host	197.204.13.7

Subnets and subnet masks

Often an entire organization is assigned only one IP network number. If the organization has several IP networks connected together with IP routers, the network manager can use subnetting to distinguish between these networks, even though they all use the same network number. Each physical network becomes a subnet with a unique subnet number.

Subnet numbers appear within IP addresses, along with network numbers and host numbers. Since an IP address is always 32 bits long, using subnet numbers means either the network number or the host numbers must use fewer bits, in order to leave room for the subnet numbers. Since the InterNIC assigns the network number proper, it should not change, so the subnet numbers must be created out of bits that would otherwise be part of the host numbers.

Subnet masks

To create subnets, the network manager must define a subnet mask, a 32-bit number that indicates which bits in an IP address are used for network and subnetwork addresses, and which are used for host addresses. One subnet mask should apply to all IP networks that are physically connected together and share a single assigned network number. Subnet masks are often written in decimal notation, like IP addresses, but they are most easily understood in binary notation. When a subnet mask is written in binary notation, each numeral 1 indicates that the corresponding bit in the IP address is part of the network or subnet address. Each 0 indicates that the corresponding bit is part of the host address. The following table shows the proper subnet masks to use for each class of network, when no subnets are required.

Class	Subnet mask for a network with no subnets
A	Binary: 11111111.00000000.00000000.00000000 Decimal: 255.0.0.0
B	Binary: 11111111.11111111.00000000.00000000 Decimal: 255.255.0.0
C	Binary: 11111111.11111111.11111111.00000000 Decimal: 255.255.255.0

To know whether subnets are being used or not, you must know what subnet mask is being used—you cannot determine this information simply from an IP address. Subnet mask information is configured as part of the process of setting up IP routers and gateways such as the Netopia R2020.

Note: If you receive a routed account from an ISP, there must be a mask associated with your network IP address. By using the IP address with the mask you can discover exactly how many IP host addresses you actually have.

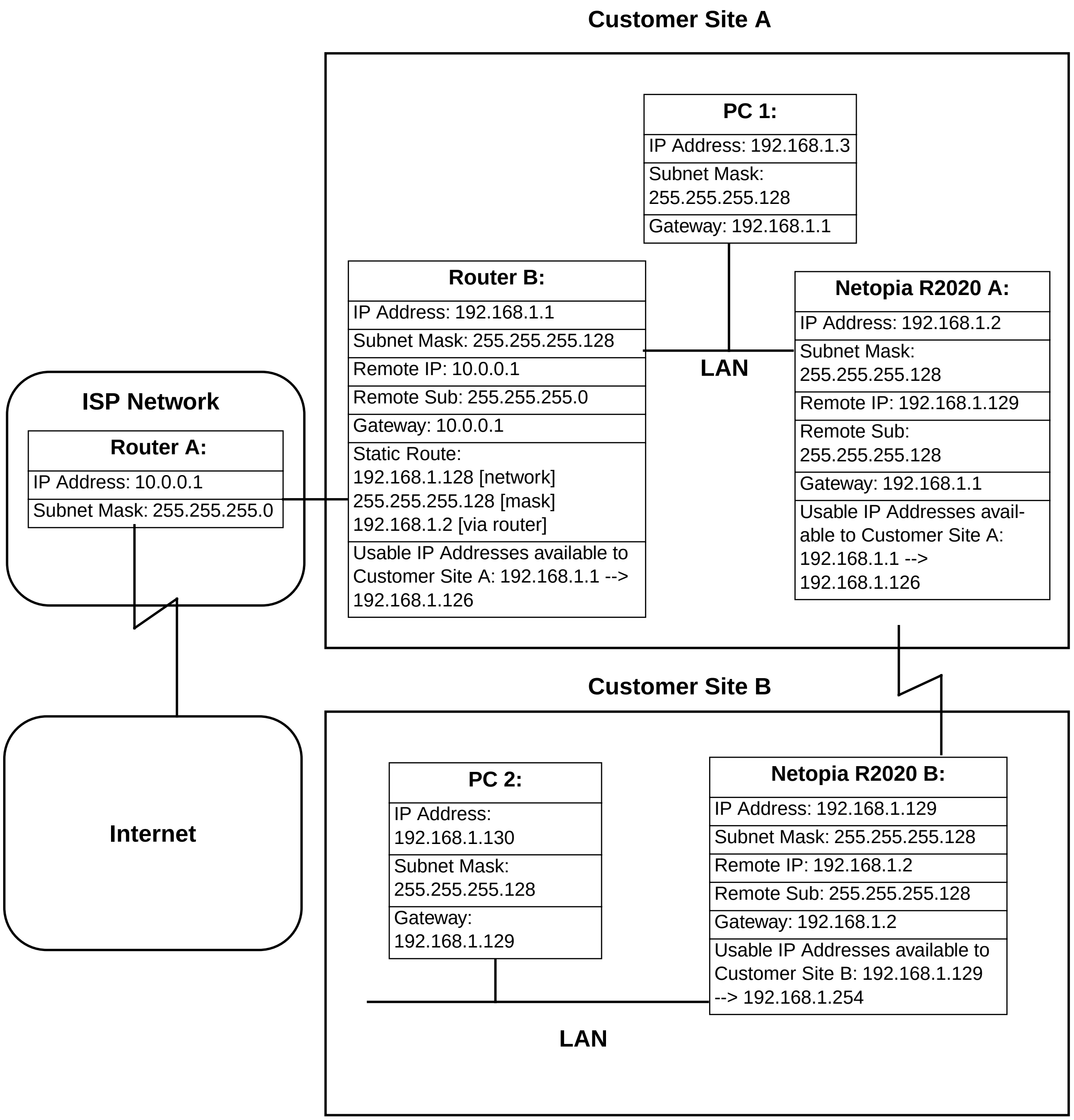
To configure subnets properly, you must also be able to convert between binary notation and decimal notation.

Example: Using subnets on a Class C IP internet

When setting up IP routing with a Class A Address, or even multiple Class C Addresses, subnetting is fairly straightforward. Subnetting a single Class C address between two networks, however, is more complex. This section describes the general procedures for subnetting a single Class C network between two Netopia routers so that each can have Internet access.

Network configuration

Below is a diagram of a simple network configuration. The ISP is providing a Class C address to the customer site, and both networks A and B want to gain Internet access through this address. Netopia R2020 B connects to Netopia R2020 A and is provided Internet access through Routers A and B.



PC 1:
IP Address: 192.168.1.3
Subnet Mask: 255.255.255.128
Gateway: 192.168.1.1

Router B:
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.128
Remote IP: 10.0.0.1
Remote Sub: 255.255.255.0
Gateway: 10.0.0.1
Static Route:
192.168.1.128 [network]
255.255.255.128 [mask]
192.168.1.2 [via router]
Usable IP Addresses available to Customer Site A: 192.168.1.1 --> 192.168.1.126

Netopia R2020 A:
IP Address: 192.168.1.2
Subnet Mask: 255.255.255.128
Remote IP: 192.168.1.129
Remote Sub: 255.255.255.128
Gateway: 192.168.1.1
Usable IP Addresses available to Customer Site A: 192.168.1.1 --> 192.168.1.126

Router A:
IP Address: 10.0.0.1
Subnet Mask: 255.255.255.0

PC 2:
IP Address: 192.168.1.130
Subnet Mask: 255.255.255.128
Gateway: 192.168.1.129

Netopia R2020 B:
IP Address: 192.168.1.129
Subnet Mask: 255.255.255.128
Remote IP: 192.168.1.2
Remote Sub: 255.255.255.128
Gateway: 192.168.1.2
Usable IP Addresses available to Customer Site B: 192.168.1.129 --> 192.168.1.254

Background

The IP Addresses and routing configurations for the devices shown in the diagram are outlined below. In addition, each individual field and its meaning are described.

The “IP Address” and “Subnet Mask” fields define the IP Address and Subnet Mask of the device's Ethernet connection to the network while the “Remote IP” and “Remote Sub” fields describe the IP Address and Subnet mask of the remote router. This information is entered in the Connection Profile of the Netopia R2020.

The “Gateway” field describes the router or workstation's default gateway or, where they will send their packets if the appropriate route is not known. The “Static Route” field, which is only shown on Router B, tells Router B what path to take to get to the network defined by Netopia R2020 B. Finally, the “Usable IP Address” field shows the range of IP Addresses available to the hosts of that network.

Note that the IP Addresses given in this section are for example purposes only. Do not use these addresses when configuring your network.

With this configuration, both Customer Site A and B can gain Internet access through Routers A and B, with no reconfiguration of the ISP's equipment. The most important item in this configuration is the Static Route defined on Router B. This tells Router B what path to take to get to the network defined by Netopia R2020 B. Without this information, Customer Site B will be able to access Customer Site A, but not the Internet.

If it is not possible to define a Static Route on Router B, RIP could be enabled to serve the same purpose. To use RIP instead of a Static Route, enable Transmit RIP on Netopia R2020 A and Transmit and Receive RIP on Router B. This will allow the route from Customer Site B to propagate on Router B and Customer Site A.

Example: Working with a Class C subnet

Suppose that your organization has a site with only 10 hosts, and no plans to add any new hosts. You don’t need a full Class C address for this site. Many ISPs offer Internet access with only a portion of a full Internet address.

For example, you may obtain the Class C address 199.14.17.48, with the mask 255.255.255.240. From the previous example, you can see that this gives you 14 host addresses to distribute to the hosts at your site. In effect, your existing network of 10 hosts is a subnet of the ISP’s network. Since the Class C address has already been reduced to subnets, you cannot further subnet your network without the risk of creating network routing problems (since you must use the mask issued by the ISP). This, however, is not a problematic limitation for your small network.

The advantages to this situation is the greater ease and lower cost of obtaining a subnet from an ISP rather than a full Class C address.

Distributing IP addresses

To set up a connection to the Internet, you may have obtained a block of IP host addresses from an Internet service provider. When configuring the Netopia R2020, you gave one of those addresses to its Ethernet port, leaving a number of addresses to distribute to computers on your network.

There are two schemes for distributing the remaining IP addresses:

- Manually give each computer an address
- Let the Netopia R2020 automatically distribute the addresses

These two methods are not mutually exclusive; you can manually issue some of the addresses while the rest are distributed by the Netopia R2020. Using the Router in this way allows it to function as an address server.

One reason to use the Netopia R2020 as an address server is that it takes less time than manually distributing the addresses. This is particularly true if you have many addresses to distribute. You only need to enter information once, rather than having to repeatedly enter it on each host separately. This also reduces the potential for misconfiguring hosts.

Another reason to use the Netopia R2020 as an address server is that it will only distribute addresses to hosts that need to use them.

All Netopia R2020s come with an integrated Dynamic Host Control Protocol (DHCP) server. Some routers also come with a Macintosh Internet Protocol (MacIP) server. These servers provide a means of distributing IP addresses to either a Mac or PC workstation as needed.

When setting up the DHCP or MacIP servers in the Netopia R2020, it is necessary to understand how workstations lease, renew, and release their IP addresses. This information will be helpful in determining dynamic address allocation for a network.

The term “lease” describes the action of a workstation requesting and using an IP address. The address is dynamic and can be returned to the address pool at a later time.

The term “renew” refers to what the workstations do to keep their leased IP address. At certain intervals, the workstation talks to the DHCP or MacIP server and renews the lease on that IP address. This renewal allows the workstation to keep and use the assigned IP address until the next renewal period.

The term “release” refers to a situation where the workstation is no longer using its assigned IP address or has been shut down. IP addresses can be manually released as well. The IP address goes back into the DHCP or MacIP address pool to be reassigned to another workstation as needed.

Technical note on subnet masking

Note: The IP address supplied by the Netopia R2020 will be a unique number. You may wish to replace this number with a number that your ISP supplies if you are configuring the router for a static IP address. The automatic IP mask supplied by SmartStart is a Class C address. However, the Netopia R2020 and all devices on the same local network must have the same subnet mask. If you require a different class address, you may edit the IP Mask field to enter the correct address. Refer to the table below.

Number of Devices (other than Netopia R2020) on Local Network	Largest Possible Ethernet Subnet Mask
1	255.255.255.252
2-5	255.255.255.248
6-13	255.255.255.240
14-29	255.255.255.224

Number of Devices (other than Netopia R2020) on Local Network	Largest Possible Ethernet Subnet Mask
30-61	255.255.255.192
62-125	255.255.255.128
125-259	255.255.255.0

Configuration

This section describes the specific IP address lease, renew, and release mechanisms for both the Mac and PC, with either DHCP or MacIP address serving.

DHCP Address Serving

Windows 95 Workstation:

- The Win95 workstation requests and renews its lease every half hour.
- The Win95 workstation does NOT relinquish its DHCP address lease when the machine is shut down.
- The lease can be manually expired using the WINIPCFG program from the Win95 machine, which is a command line program executable from the DOS prompt or from the START:RUN menu.

Windows 3.1 Workstation (MSTCP Version 3.11a):

- The Win3.1 workstation requests and renews its lease every half hour.
- The Win3.1 workstation does NOT relinquish its DHCP address lease when the user exits Windows and goes to DOS.
- The lease can be manually expired by typing IPCONFIG /RELEASE from a DOS window within Windows or from the DOS prompt.</UL>

Macintosh Workstation (Open Transport Version 1.1 or later):

- The Mac workstation requests and renews its lease every half hour.
- The Mac workstation will relinquish its address upon shutdown in all but one case. If the TCP/IP control panel is set to initialize at start-up, and no IP services are used or the TCP/IP control panel is not opened, the DHCP address will NOT be relinquished upon shutdown. However, if the TCP/IP control panel is opened, or if an IP application is used, the Mac WILL relinquish the lease upon shutdown.
- If the TCP/IP control panel is set to acquire an address only when needed (therefore a TCP/IP application must have been launched to obtain a lease) the Mac WILL relinquish its lease upon shutdown every time.

Netopia R2020 DHCP Server Characteristics

- The Netopia R2020 ignores any lease-time associated with a DHCP request and automatically issues the DHCP address lease for one hour.
- The number of devices a Netopia R2020 can serve DHCP to is 512. This is imposed by global limits on the size of the address serving database, which is shared by all address serving functions active in the router.
- The Netopia R2020 does release the DHCP address back to the available DHCP address pool precisely

one hour after the last heard lease request as some other DHCP implementations may hold on to the lease for an additional time after the lease expired, to act as a buffer for variances in clocks between the client and server.

MacIP Serving

Macintosh Workstation (MacTCP or Open Transport):

Once the Mac workstation requests and receives a valid address, the Netopia R2020 will actively check for the workstation’s existence once every minute.

- For a DYNAMIC address, the Netopia R2020 will release the address back to the address pool after it has lost contact with the Mac workstation for over 2 minutes.
- For a STATIC address, the Netopia R2020 will release the address back to the address pool after it has lost contact with the Mac workstation for over 20 minutes.

Netopia R2020 MacIP Server Characteristics

The Mac workstation uses ATP to both request and receive an address from the Netopia R2020's MacIP server. Once acquired, NBP confirm packets will be sent out every minute from the Netopia R2020 to the Mac workstation.

Manually distributing IP addresses

If you choose to manually distribute IP addresses, you must enter each computer’s address into its TCP/IP stack software. Once you manually issue an address to a computer, it possesses that address until you manually remove it. That’s why manually distributed addresses are sometimes called static addresses.

Static addresses are useful in cases when you want to make sure that a host on your network cannot have its address taken away by the address server. A network administrator’s computer, a computer dedicated to communicating with the Internet, and routers are appropriate candidates for a static address.

Using address serving

The Netopia R2020 provides three ways to serve IP addresses to computers on a network. The first, Dynamic Host Configuration Protocol (DHCP), is supported by PCs with Microsoft Windows and a TCP/IP stack. Macintosh computers using Open Transport and computers using the UNIX operating system may also be able to use DHCP. The second way, MacIP, is for Macintosh computers. The third way, called Serve Dynamic WAN Clients (IPCP), is used to fulfill WAN client requirements

The Netopia R2020 can use both DHCP and MacIP. Whether you use one or both will depend on your particular networking environment. If that environment includes both PCs and Macintosh computers that do not use Open Transport, you will need to use both DHCP and MacIP to distribute IP addresses to all of your computers.

Serve dynamic WAN clients

The third method, used to fulfill WAN client requirements, is called Serve Dynamic WAN Clients. This is a subset of PPP. Originally, this would apply only to switched WAN interface routers, and not to leased line routers. However, a new feature can give you Asynchronous PPP dial-in support on the Auxiliary port on any router including leased line Netopia routers.

In any situation where a device is dialing into a Netopia router, the router may need to be configured to serve IP via the WAN interface. This is only a requirement if the calling device has not been configured locally to know what its address(es) are. So when a client, dialing into a Netopia router's WAN interface, is expecting addresses to be served by the answering router, you must set the answering Netopia router to serve IP via its WAN interface.

You can do this in either of two ways:

- use the Serve Dynamic WAN Clients option in the Address Serving Setup screen.

  Serve Dynamic WAN Clients enabled only allows you to specify a pool of addresses from which the dial-in client may get an IP address. It does not allow static addressing.

  If you want to serve addresses dynamically, use Serve Dynamic WAN Clients.

- define the address that you want to serve in the Connection Profile's IP Setup screen.

  This method requires a static value to be used. Thus any user dialing in can obtain the same IP address for every connection to the profile.

  If you want to serve addresses statically, define the address in the Connection Profile.

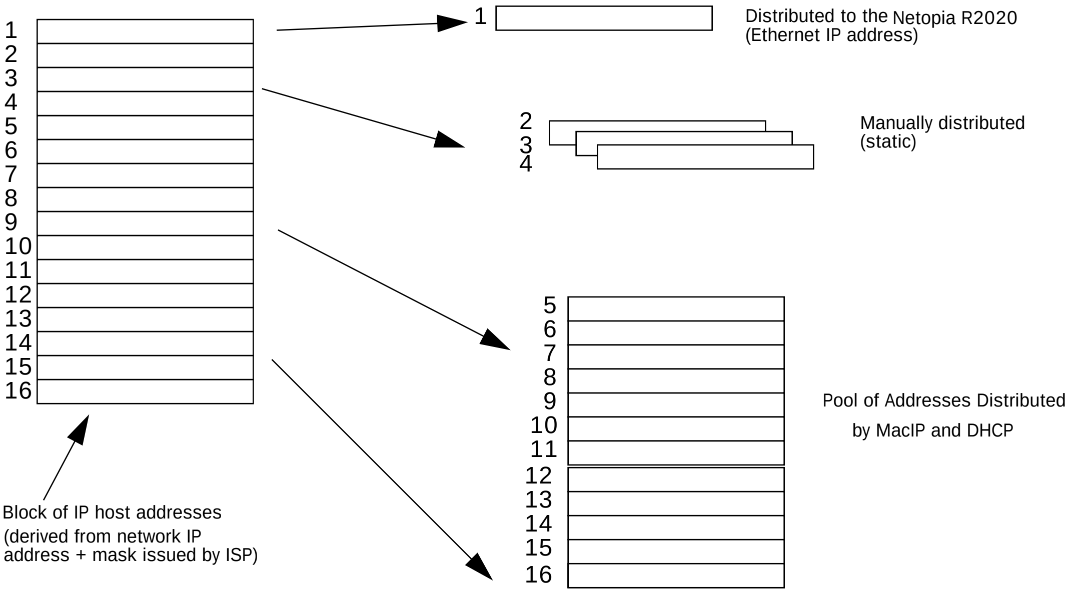
  Notes:

  - The addresses that are to be served cannot be used elsewhere. For example you wouldn't want to define a static address in a Connection Profile to be served via the WAN that is already defined in the DHCP pool of addresses.
  - In order to work correctly, you must define a “host” or “node” address in the IP Profile Parameters of the Connection Profile.

    This is accomplished by specifying the IP address that is to be statically served via the WAN, and then by entering a mask value of 255.255.255.255.

Tips and rules for distributing IP addresses

- Before you allocate IP addresses using DHCP and MacIP, consider whether you need to set aside any static addresses.
- Note any planned and currently used static addresses before you use DHCP and MacIP.
- Avoid fragmenting your block of IP addresses. For example, try to use a continuous range for the static addresses you choose.


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
Block of IP host addresses
(derived from network IP address + mask issued by ISP)
1
Distributed to the Netopia R2020
(Ethernet IP address)
2
3
4
Manually distributed
(static)
5
6
7
8
9
10
11
12
13
14
15
16
Pool of Addresses Distributed
by MacIP and DHCP

The figure above shows an example of a block of IP addresses being distributed correctly.

The example follows these rules:

- An IP address must not be used as a static address if it is also in a range of addresses being distributed by DHCP or MacIP.
- A single IP address range is used by all the address-served clients. These include DHCP, BOOTP, MacIP, and WAN clients, even though BOOTP and static MacIP clients might not be considered served.
- The address range specified for address-served clients cannot wrap around from the end of the total available range back to the beginning. See below for a further explanation and an example.
- The network address issued by an ISP cannot be used as a host address.

A DHCP example

Suppose, for example, that your ISP gave your network the IP address 199.1.1.32, and a 4-bit subnet mask. Address 199.1.1.32 is reserved as the network address. Address 199.1.1.47 is reserved as the broadcast address. This leaves 14 addresses to allocate, from 199.1.1.33 through 199.1.1.46. If you want to allocate a sub-block of 10 addresses using DHCP, enter “10” in the DHCP Setup screen’s **Number of Addresses to Allocate** item. Then, in the same screen’s **First Address** item, enter the first address in the sub-block to allocate such that all 10 addresses are within your original block. You could enter 199.1.1.33, or 199.1.1.37, or any address between them. Note that if you entered 199.1.1.42 as the first address, network routing errors would probably result because you would be using a range with addresses that do not belong to your network (199.1.1.49, 199.1.1.50, and 199.1.1.51).

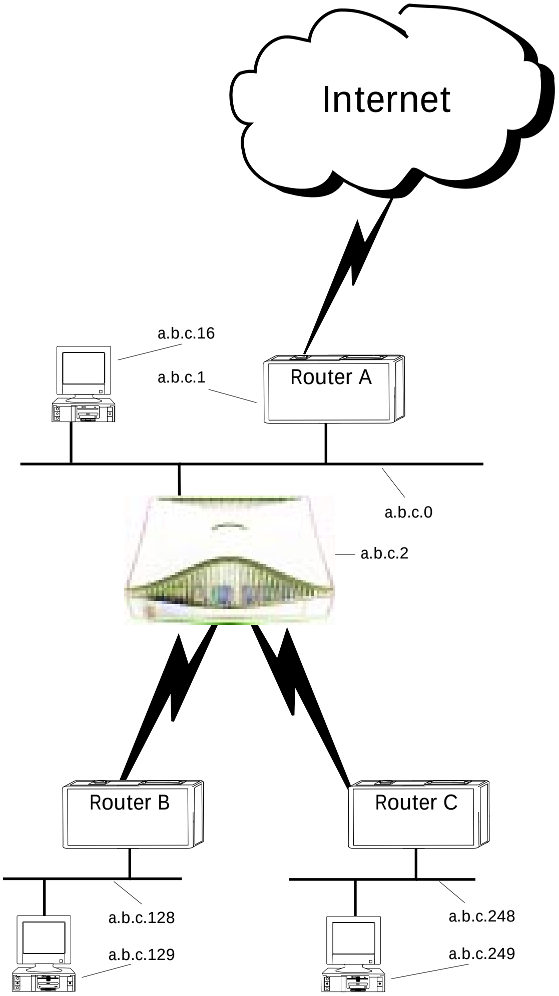
Nested IP subnets

Under certain situations, you may wish to create remote subnets from the limited number of IP addresses issued by your ISP or other authority. You can do this using connection profiles. These subnets can be nested within the range of IP addresses available to your network.

For example, suppose that you obtain the Class C network address a.b.c.0 to be distributed among three networks. This network address can be used on your main network while portions of it can be subnetted to the two remaining networks.

Note: The IP address a.b.c.0 has letters in place of the first three numbers to generalize it for this example.

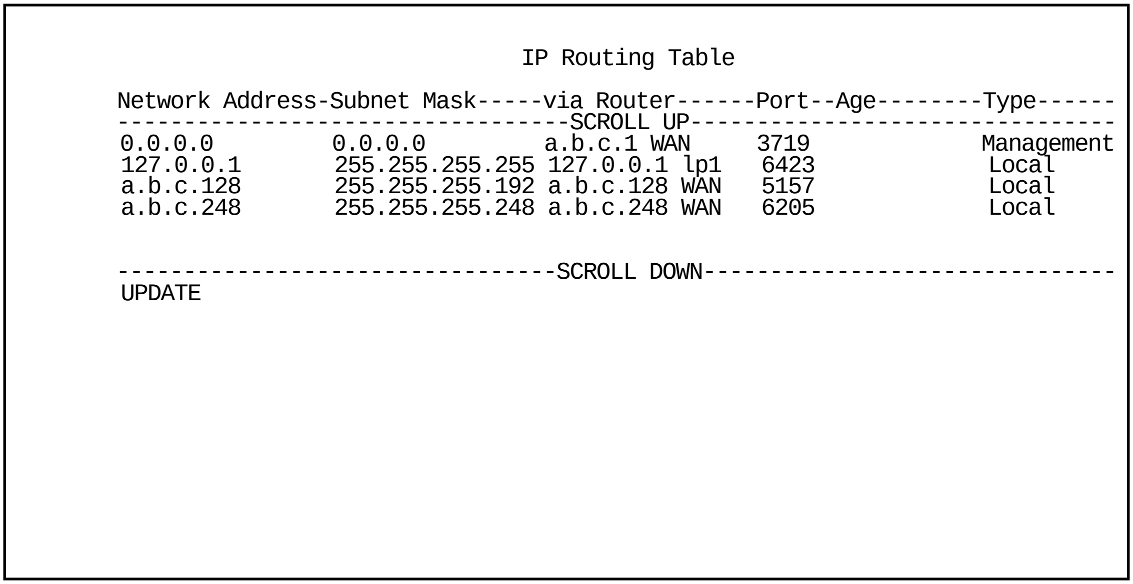
The figure at left shows a possible network configuration following this scheme. The main network is set up with the Class C address a.b.c.0, and contains Router A (which could be a Netopia R2020), a Netopia R2020, and a number of other hosts. Router A maintains a link to the Internet, and may be used as the default gateway.



Routers B and C (which could also be Netopia R2020s) serve the two remote networks that are subnets of a.b.c.0. The subnetting is accomplished by configuring the Netopia R2020 with connection profiles for Routers B and C (see the following table).

Connection profile	Remote IP address	Remote IP mask	Bits available for host address
for Router B	a.b.c.128	255.255.255.192	7
for Router C	a.b.c.248	255.255.255.248	3

The Netopia R2020's connection profiles for Routers B and C create entries in its IP routing table. One entry points to the subnet a.b.c.128, while a second entry points to the subnet a.b.c.248. The IP routing table might look similar to the following:



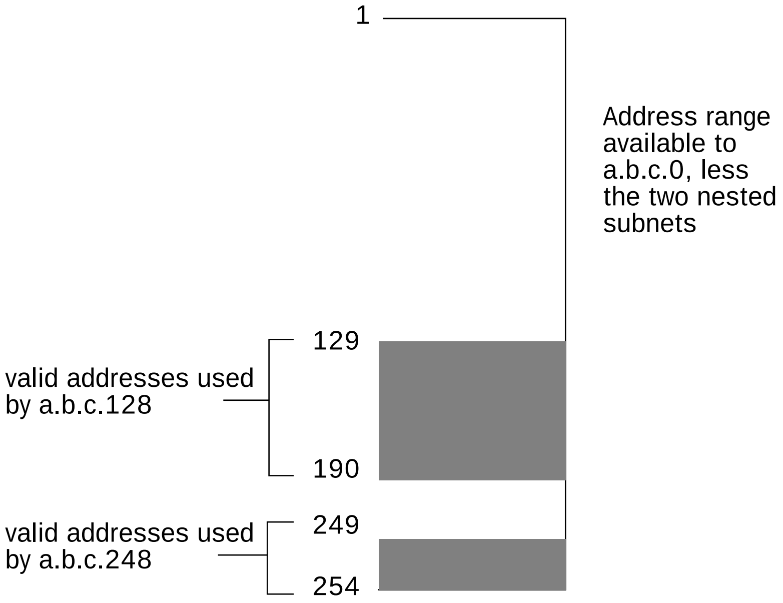
```
                                IP Routing Table

Network Address-Subnet Mask-----via Router------Port--Age--------Type------
----------------------------------SCROLL UP--------------------------------
0.0.0.0         0.0.0.0         a.b.c.1 WAN     3719             Management
127.0.0.1       255.255.255.255 127.0.0.1 lp1   6423             Local
a.b.c.128       255.255.255.192 a.b.c.128 WAN   5157             Local
a.b.c.248       255.255.255.248 a.b.c.248 WAN   6205             Local


---------------------------------SCROLL DOWN-------------------------------
UPDATE
```

Let's see how a packet from the Internet gets routed to the host with IP address a.b.c.249, which is served by Router C. The packet first arrives at Router A, which delivers it to its local network (a.b.c.0). The packet is then received by the Netopia R2020, which examines its destination IP address.

The Netopia R2020 compares the packet's destination IP address with the routes in its IP routing table. It begins with the route at the bottom of the list and works up until there's a match or the route to the default gateway is reached.

When a.b.c.249 is masked by the first route's subnet mask, it yields a.b.c.248, which matches the network address in the route. The Netopia R2020 uses the connection profile associated with the route to connect to Router C, and then forwards the packet. Router C delivers the packet to the host on its local network.

The following diagram illustrates the IP address space taken up by the two remote IP subnets. You can see from the diagram why the term nested is appropriate for describing these subnets.


1
Address range available to a.b.c.0, less the two nested subnets
valid addresses used by a.b.c.128
129
190
valid addresses used by a.b.c.248
249
254

Broadcasts

As mentioned earlier, binary IP host or subnet addresses composed entirely of ones or zeros are reserved for broadcasting. A broadcast packet is a packet that is to be delivered to every host on the network, if both the host address and the subnet address are all ones or all zeros, or to every host on the subnetwork, if the host address is all ones or all zeros but the subnet address is a combination or zeros and ones. Instead of making many copies of the packet, individually addressed to different hosts, all the host machines know to pay attention to broadcast packets, as well as to packets addressed to their specific individual host addresses. Depending on the age and type of IP equipment you use, broadcasts will be addressed using either all zeros or all ones, but not both. If your network requires zeros broadcasting, you must configure this through SNMP.

Packet header types

As previously mentioned, IP works with other protocols to allow communication over IP networks. When IP is used on an Ethernet network, IP works with the Ethernet or 802.3 framing standards, among other protocols. These two protocols specify two different ways to organize the very first signals in the sequence of electrical signals that make up an IP packet travelling over Ethernet. By default, the Netopia R2020 uses Ethernet packet headers for IP traffic. If your network requires 802.3 IP framing, you must configure this through SNMP.

Appendix D

Binary Conversion Table

This table is provided to help you choose subnet numbers and host numbers for IP and MacIP networks that use subnetting for IP addresses.

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
0	0	32	100000	64	1000000	96	1100000
1	1	33	1000001	65	1000001	97	1100001
2	10	34	100010	66	1000010	98	1100010
3	11	35	100011	67	1000011	99	1100011
4	100	36	100100	68	1000100	100	1100100
5	101	37	100101	69	1000101	101	1100101
6	110	38	100110	70	1000110	102	1100110
7	111	39	100111	71	1000111	103	1100111
8	1000	40	101000	72	1001000	104	1101000
9	1001	41	101001	73	1001001	105	1101001
10	1010	42	101010	74	1001010	106	1101010
11	1011	43	101011	75	1001011	107	1101011
12	1100	44	101100	76	1001100	108	1101100
13	1101	45	101101	77	1001101	109	1101101
14	1110	46	101110	78	1001110	110	1101110
15	1111	47	101111	79	1001111	111	1101111
16	10000	48	110000	80	1010000	112	1110000
17	10001	49	110001	81	1010001	113	1110001
18	10010	50	110010	82	1010010	114	1110010
19	10011	51	110011	83	1010011	115	1110011
20	10100	52	110100	84	1010100	116	1110100
21	10101	53	110101	85	1010101	117	1110101
22	10110	54	110110	86	1010110	118	1110110
23	10111	55	110111	87	1010111	119	1110111
24	11000	56	111000	88	1011000	120	1111000
25	11001	57	111001	89	1011001	121	1111001
26	11010	58	111010	90	1011010	122	1111010
27	11011	59	111011	91	1011011	123	1111011
28	11100	60	111100	92	1011100	124	1111100
29	11101	61	111101	93	1011101	125	1111101
30	11110	62	111110	94	1011110	126	1111110
31	11111	63	111111	95	1011111	127	1111111

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
128	10000000	160	10100000	192	11000000	224	11100000
129	10000001	161	10100001	193	11000001	225	11100001
130	10000010	162	10100010	194	11000010	226	11100010
131	10000011	163	10100011	195	11000011	227	11100011
132	10000100	164	10100100	196	11000100	228	11100100
133	10000101	165	10100101	197	11000101	229	11100101
134	10000110	166	10100110	198	11000110	230	11100110
135	10000111	167	10100111	199	11000111	231	11100111
136	10001000	168	10101000	200	11001000	232	11101000
137	10001001	169	10101001	201	11001001	233	11101001
138	10001010	170	10101010	202	11001010	234	11101010
139	10001011	171	10101011	203	11001011	235	11101011
140	10001100	172	10101100	204	11001100	236	11101100
141	10001101	173	10101101	205	11001101	237	11101101
142	10001110	174	10101110	206	11001110	238	11101110
143	10001111	175	10101111	207	11001111	239	11101111
144	10010000	176	10110000	208	11010000	240	11110000
145	10010001	177	10110001	209	11010001	241	11110001
146	10010010	178	10110010	210	11010010	242	11110010
147	10010011	179	10110011	211	11010011	243	11110011
148	10010100	180	10110100	212	11010100	244	11110100
149	10010101	181	10110101	213	11010101	245	11110101
150	10010110	182	10110110	214	11010110	246	11110110
151	10010111	183	10110111	215	11010111	247	11110111
152	10011000	184	10111000	216	11011000	248	11111000
153	10011001	185	10111001	217	11011001	249	11111001
154	10011010	186	10111010	218	11011010	250	11111010
155	10011011	187	10111011	219	11011011	251	11111011
156	10011100	188	10111100	220	11011100	252	11111100
157	10011101	189	10111101	221	11011101	253	11111101
158	10011110	190	10111110	222	11011110	254	11111110
159	10011111	191	10111111	223	11011111	255	11111111

Appendix E

Further Reading

Angell, David. *ISDN for Dummies*, Foster City, CA: IDG Books Worldwide, 1995. Thorough introduction to ISDN for beginners.

Apple Computer, Inc. *AppleTalk Network System Overview*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1989.

Apple Computer, Inc. *Planning and Managing AppleTalk Networks*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1991.

Black, U. *Data Networks: Concepts, Theory and Practice*. Englewood Cliffs, New Jersey: Prentice Hall; 1989.

Black, U. *Physical Level Interfaces and Protocols*. Los Alamitos, California: IEEE Computer Society Press; 1988.

Black, Uyless. *Emerging Communications Technologies*, Englewood Cliffs, New Jersey: PTR Prentice Hall, 1994. Describes how emerging communications technologies, including ISDN and Frame Relay operate and where they fit in a computer/communications network.

Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall. "Network Management and the Design of SNMP." ConneXions: The Interoperability Report, Vol. 3: March 1989.

Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall. "Introduction to the Simple Gateway Monitoring Protocol." IEEE Network: March 1988."

Chapman, D. Brent and Elizabeth D. Zwicky. *Building Internet Firewalls*, Sebastopol, CA: O'Reilly & Associates, 1995. Dense and technical, but Chapter 6 provides a basic introduction to packet filtering.

Chapman, D. Brent. "Network (In)Security Through IP Packet Filtering," paper available from Great Circle Associates, 1057 West Dana Street, Mountain View, CA 94041

Chappell, L. *Novell's Guide to NetWare LAN Analysis*. San Jose, California: Novell Press; 1993.

Clark, W. "SNA Internetworking." ConneXions: The Interoperability Report, Vol. 6, No. 3: March 1992.

Coltun, R. "OSPF: An Internet Routing Protocol." ConneXions: The Interoperability Report, Vol. 3, No. 8: August 1989.

Comer, D.E. *Internetworking with TCP/IP: Principles, Protocols, and Architecture*, Vol. I, 2nd ed. Englewood Cliffs, New Jersey: Prentice Hall; 1991.

Davidson, J. *An Introduction to TCP/IP*. New York, New York: Springer-Verlag; 1992.

Ferrari, D. *Computer Systems Performance Evaluation*. Englewood Cliffs, New Jersey: Prentice Hall; 1978.

Garcia-Luna-Aceves, J.J. "Loop-Free Routing Using Diffusing Computations." Publication pending in IEEE/ACM Transactions on Networking, Vol. 1, No. 1, 1993.

Garfinkel, Simson. *PGP: Pretty Good Privacy*, Sebastopol, CA: O'Reilly & Associates, 1991. A guide to the free data encryption program PGP and the issues surrounding encryption.

Green, J.K. *Telecommunications*, 2nd ed. Homewood, Illinois: Business One Irwin; 1992.

Hagans, R. "Components of OSI: ES-IS Routing." ConneXions: The Interoperability Report, Vol. 3, No. 8: August 1989.

Hares, S. "Components of OSI: Inter-Domain Routing Protocol (IDRP)." ConneXions: The Interoperability Report, Vol. 6, No. 5: May 1992.

Jones, N.E.H. and D. Kosiur. *Macworld Networking Handbook*. San Mateo, California: IDG Books Worldwide, Inc.; 1992.

Joyce, S.T. and J.Q. Walker II. "Advanced Peer-to-Peer Networking (APPN): An Overview." ConneXions: The Interoperability Report, Vol. 6, No. 10: October 1992.

Kousky, K. "Bridging the Network Gap." LAN Technology, Vol. 6, No. 1: January 1990.

LaQuey, Tracy. *The Internet Companion: A Beginner's Guide to Global Networking*, Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1994.

Leinwand, A. and K. Fang. *Network Management: A Practical Perspective*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1993.

Levine, John R. and Carol Baroudi. *The Internet for Dummies*, Foster City, CA: IDG Books Worldwide, 1993. Covers all of the most popular Internet services, including e-mail, newsgroups, and the World Wide Web. Also has information on setting up individual workstations with TCP/IP stacks.

Lippis, N. "The Internetwork Decade." Data Communications, Vol. 20, No. 14: October 1991.

McNamara, J.E. *Local Area Networks*. Digital Press, Educational Services, Digital Equipment Corporation, 12 Crosby Drive, Bedford, MA 01730.

Malamud, C. *Analyzing DECnet/OSI Phase V*. New York, New York: Van Nostrand Reinhold; 1991.

Malamud, C. *Analyzing Novell Networks*. New York, New York: Van Nostrand Reinhold; 1991.

Malamud, C. *Analyzing Sun Networks*. New York, New York: Van Nostrand Reinhold; 1991.

Martin, J. *SNA: IBM's Networking Solution*. Englewood Cliffs, New Jersey: Prentice Hall; 1987.

Martin, J., with K.K. Chapman and the ARBEN Group, Inc. *Local Area Networks. Architectures and Implementations*. Englewood Cliffs, New Jersey: Prentice Hall; 1989.

Medin, M. "The Great IGP Debate--Part Two: The Open Shortest Path First (OSPF) Routing Protocol." ConneXions: The Interoperability Report, Vol. 5, No. 10: October 1991.

Meijer, A. *Systems Network Architecture: A tutorial*. New York, New York: John Wiley & Sons, Inc.; 1987.

Miller, A. Mark. *Analyzing Broadband Networks (Frame Relay, SMDS, & ATM)*, M&T Books: A Division of MIS: Press, 1994. An intermediate/advanced reference on Frame Relay technologies.

Miller, M.A. *Internetworking: A Guide to Network Communications* LAN to LAN; LAN to WAN, 2nd. ed. San Mateo, California: M&T Books; 1992.

Miller, M.A. *LAN Protocol Handbook*. San Mateo, California: M&T Books; 1990.

Miller, M.A. *LAN Troubleshooting Handbook*. San Mateo, California: M&T Books; 1989.

O'Reilly, T. and G. Todino. *Managing UUCP and Usenet, 10th ed.* Sebastopol, California: O'Reilly & Associates, Inc.; 1992.

Perlman, R. *Interconnections: Bridges and Routers*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1992.

Perlman, R. and R. Callon. "The Great IGP Debate--Part One: IS-IS and Integrated Routing." ConneXions: The Interoperability Report, Vol. 5, No. 10: October 1991.

Rose, M.T. *The Open Book: A Practical Perspective on OSI*. Englewood Cliffs, New Jersey: Prentice Hall; 1990.

Rose, M.T. *The Simple Book: An Introduction to Management of TCP/IP-based Internets*. Englewood Cliffs, New Jersey: Prentice Hall; 1991.

Ross, F.E. "FDDI--A Tutorial." IEEE Communications Magazine, Vol. 24, No. 5: May 1986.

Schlar, S.K. *Inside X.25: A Manager's Guide*. New York, New York: McGraw-Hill, Inc.; 1990.

Schwartz, M. *Telecommunications Networks: Protocols, Modeling, and Analysis*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1987.

Sherman, K. *Data Communications: A User's Guide*. Englewood Cliffs, New Jersey: Prentice Hall; 1990.

Sidhu, G.S., R.F. Andrews, and A.B. Oppenheimer. *Inside AppleTalk, 2nd ed.* Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1990.

Siyan, Karanjit. *Internet Firewall and Network Security*, Indianapolis: New Riders Publishing, 1995. Similar to the Chapman and Zwicky book.

Smith, Philip. *Frame Relay Principles and Applications*, Addison-Wesley Publishing Company, 1996. Covers information on Frame Relay, including the pros and cons of the technology, description of the theory and application, and an explanation of the standardization process.

Spragins, J.D. et al. *Telecommunications Protocols and Design*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1991.

Stallings, W. *Data and Computer Communications*. New York, New York: Macmillan Publishing Company; 1991.

Stallings, W. *Handbook of Computer-Communications Standards,* Vols. 1-3. Carmel, Indiana: Howard W. Sams, Inc.; 1990.

Stallings, W. *Local Networks*, 3rd ed. New York, New York: Macmillan Publishing Company; 1990.

Stevens, W.R. *TCP/IP Illustrated*, Vol 1. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1994.

Sunshine, C.A. (ed.). *Computer Network Architectures and Protocols*, 2nd ed. New York, New York: Plenum Press; 1989.

Tannenbaum, A.S. *Computer Networks*, 2nd ed. Englewood Cliffs, New Jersey: Prentice Hall; 1988.

Terplan, K. *Communication Networks Management*. Englewood Cliffs, New Jersey: Prentice Hall; 1992.

Tsuchiya, P. "Components of OSI: IS-IS Intra-Domain Routing." ConneXions: The Interoperability Report, Vol. 3, No. 8: August 1989.

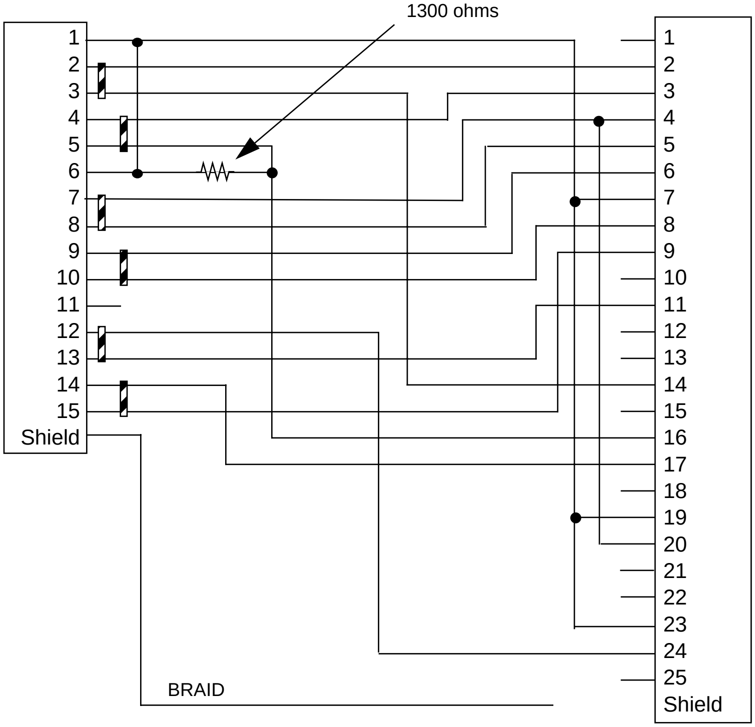
Tsuchiya, P. "Components of OSI: Routing (An Overview)." ConneXions: The Interoperability Report, Vol. 3, No. 8: August 1989.

Zimmerman, H. "OSI Reference Model--The ISO Model of Architecture for Open Systems Interconnection." IEEE Transactions on Communications COM-28, No. 4: April 1980.

Appendix F

Technical Specifications and Safety Information

Pinouts for Auxiliary Port Modem Cable



HD-15		DB-25	
Pin 1	Ground	Pin 1	(not used)
Pin 2	TDA	Pin 2	TD
Pin 3	TDB	Pin 3	RD
Pin 4	RDA	Pin 4	RTS
Pin 5	RDB	Pin 5	CTS
Pin 6	(not used)	Pin 6	DCE Ready
Pin 7	DTR	Pin 7	Ground
Pin 8	CTS	Pin 8	RLSD

HD-15		DB-25	
Pin 9	DSR	Pin 9	-RSET (EIA-530)
Pin 10	DCD	Pin 10	(not used)
Pin 11	(not used)	Pin 11	-TSET (EIA-530)
Pin 12	TCA	Pin 12	(not used)
Pin 13	TCB	Pin 13	(not used)
Pin 14	RCA	Pin 14	-TD (EIA-530) STD (EIA-232)
Pin 15	RCB	Pin 15	(not used)
		Pin 16	-RD (EIA-530) SRD (EIA-232)
		Pin 17	RSET
		Pin 18	(not used)
		Pin 19	-RTS (EIA-530) SRTS (EIA-232)
		Pin 20	DTE Ready
		Pin 21	(not used)
		Pin 22	(not used)
		Pin 23	Ground
		Pin 24	TSET
		Pin 25	(not used)
Note: Certain RS-232 modems do not properly accept signals on pins 12/24, 13/11, 14/17, and 15/9. For these applications, these pins may need to be cut.			

Description

Dimensions: 124.0 cm (w) x 20.0 cm (d) x 5.3 cm (h)
9.4” (w) x 7.9” (d) x 2.1” (h)

Communications interfaces: The Netopia R2020 Dual Analog Router has two RJ-45 jacks for modem connections; an 8 port 10Base-T Ethernet hub for your LAN connection; a DE-9 Console port; and an HD-15 Auxiliary port that can be used as either a serial or LocalTalk port.

56K Modem Specifications: complies with ITU-T V.90 and/or K56flex standard

Power requirements

- 12 VDC input
- 1.5 Amps

Environment

Operating temperature: 0° to +40° C

Storage temperature: 0° to +70° C

Relative storage humidity: 20 to 80% non-condensing

Software and protocols

Software media: Software preloaded on internal flash memory; field upgrades done via download to internal flash memory via XMODEM or TFTP

Routing: TCP/IP Internet Protocol Suite, RIP, AppleTalk*, LocalTalk-to-Ethernet routing*, AURP tunneling*, MacIP*, IPX

* optional add-on feature

WAN support: PPP, MP, HDLC

Security: PAP, CHAP, PAP-TOKEN, CACHE-TOKEN, callback, SecurID, IP/IPX firewalls, UI password security, and CallerID

SNMP network management: SNMPv1, MIB-II (RFC 1213), Interface MIB (RFC 1229), Ethernet MIB (RFC 1643), AppleTalk MIB-I (1243), Netopia R2020 MIB

Management/configuration methods: HTTP (web server), serial console, remote modem console, telnet, SNMP

Diagnostics: PING, event logging, routing table displays, traceroute, statistics counters, Call Accounting

Agency approvals

The Netopia R2020 Dual Analog Router has met the safety standards (per CSA-950) of the Canadian Standards Association for Canada.

The Netopia R2020 Dual Analog Router has met the safety standards (per UL-1950) of the Underwriters Laboratories for United States.

Regulatory notices

Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. Adequate measures include increasing the physical distance between this product and other electrical devices.

United States. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Requirements, Part 68. The Federal Communications Commission (FCC) has established Rules which permit this device to be directly connected to the telephone network. Standardized jacks are used for these connections. This equipment should not be used on party lines or coin phones.

If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until repair has been made. If this is not done, the telephone company may temporarily disconnect service.

The telephone company may make changes in its technical operations and procedures; if such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes. You will be advised of your right to file a complaint with the FCC.

If the telephone company requests information on what equipment is connected to their lines, inform them of:

a) The telephone number to which this unit is connected.

b) The ringer equivalence number

c) The USOC jack required. (RJ11C)

d) The FCC Registration Number. (14 digits provided by FCC)

Items (b) and (d) are indicated on the label. The Ringer Equivalence Number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the REN's of all devices on any one line should not exceed five (5.0). If too many devices are attached, they many not ring properly.

Service Requirements. In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. Under FCC rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or our of warranty. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents. Service can be obtained at Netopia, Inc., 2470 Mariner Square Loop, Alameda, California, 94501.

Important

This product was tested for FCC compliance under conditions that included the use of shielded cables and connectors between system components. Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment.

Canada. This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Declaration for Canadian users

The Canadian Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord.) The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to the certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all the devices does not exceed 100.

Important safety instructions

Caution

- The direct plug-in power supply serves as the main power disconnect; locate the direct plug-in power supply near the product for easy access.
- For use only with CSA Certified Class 2 power supply, rated 12VDC, 1.5A.

Telecommunication installation cautions

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.

Battery

The Netopia R2020’s lithium battery is designed to last for the life of the product. The battery is not user-serviceable.

Caution!

Danger of explosion if battery is incorrectly replaced.

Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

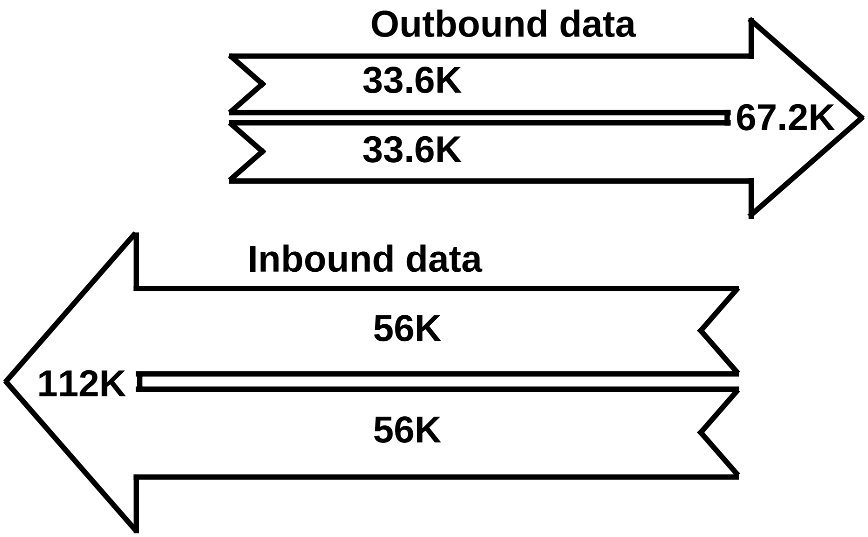
Appendix G

About 56K Line Access

The Netopia R2020 is capable of 56Kbps per line connections. This means that if you use both onboard modems, you can achieve inbound data transfer rates of up to 112Kbps. Using a third modem bumps the theoretical speed limit to 168Kbps.

This section describes some practical limitations on the previous statements.

A current FCC limitation will only permit a maximum speed of 52Kbps over analog phone lines using combined analog/digital technology. Also, the data transfer rates are for *inbound* data only. Outbound data is limited to the current transfer rates for analog phone lines alone which is 33.6Kbps. So, using both onboard modems under optimal conditions, will yield an inbound data transfer rate of 104Kbps and an outbound rate of 67.2Kbps. This means that your incoming email, file transfers and downloads, web browsing, and so on, occur at 104Kbps, while your outgoing information, such as outbound email, travels at 67.2Kbps. With a third modem, the rates become 156Kbps inbound and 100.8Kbps outbound. Also, to achieve the maximum inbound rates, the ISP-side data must be digitally sourced.



Above a certain threshold (called Shannon's Limit) the signal-to-noise ratio of any medium becomes too low to reliably transfer data. The analog phone line is the limiting factor in the speed of data transmission because of the inherent noise it contributes.

Today's telephone network is increasingly digital. In particular, the portion of the phone connection between the phone company and the Internet Service Provider (ISP) is often digital. Digital lines still have noise, and are still subject to Shannon's limit, but they have less noise and a higher ceiling.

Several companies have created techniques that take advantage of the digital portion of the phone network to achieve higher speeds than were possible with a purely analog pathway.

These new techniques treat the phone system as a mostly digital network that just happens to have an analog portion. There are several consequences to the reliance on a half-digital connection. Your Internet Service Provider must have digital phone lines to the public switched telephone network (PSTN). That's the easy part: if your ISP offers 56Kbps, they have the digital lines.

Getting the most out of 56K technology requires that you have optimal conditions on your telephone line. Any noise in the line will degrade your connection. Statistics show that most people connect somewhere between 45 and 50K. Many connect at 52K. Connect rates between 40 and 50K are in no way a failure on the part of the Internet Service Provider, but simply a fact of life in trying to extend the limitations of noisy analog telephone lines.

The Netopia R2020 ships with the unified ITU V.90 standard firmware, also known as V.PCM, which merges the K56flex standard with the competing x2 standard. Modem firmware updates that may from time to time become available will be made available on the Netopia website. See "Transferring configuration and firmware files with TFTP," and "Transferring configuration and firmware files with XMODEM," in Chapter 15, "Utilities and Diagnostics."

Glossary

Access Line: A telephone line reaching from the telephone company central office to a point usually on your premises. Beyond this point the wire is considered inside wiring. See also *Trunk Line*.

analog: In telecommunications, telephone transmission and/or switching that is not digital. An analog phone transmission is one that was originally intended to carry speech or voice, but may with appropriate modifications be used to carry data of other types.

ANSI (American National Standards Institute): Devises and proposes recommendations for international communications standards. See also *Comite Consultatif International Telegraphique et Telephonique (CCITT*).

AppleTalk: A comprehensive network system designed and developed by Apple Computer, Inc. AppleTalk allows many different types of computer systems, printers, and servers to communicate on a variety of cabling schemes, including LocalTalk and Ethernet cabling. In this manual, AppleTalk refers especially to the protocols or rule sets that govern this communication.

AppleTalk address: A unique identifier for each device using AppleTalk that allows information to be sent and received correctly. An AppleTalk address always includes a network number wherever two or more AppleTalk networks are connected together by routers.

AURP (Apple Update-based Router Protocol): An enhanced AppleTalk routing protocol. AURP provides improved support for AppleTalk over wide area networks (WANs) and tunneling through non-AppleTalk (IP) networks. AURP features include network number remapping, clustering of remote network numbers, and hop count reduction.

backbone: A network topology consisting of a single length of cable with multiple network connection points.

Bandwidth: The range of frequencies, expressed in Kilobits per second, that can pass over a given data transmission channel within a network. The bandwidth determines the rate at which information can be sent through a channel - the greater the bandwidth, the more information that can be sent in a given amount of time.

BAP: Bandwidth Allocation Protocol. Manages the dynamic bandwidth allocation of implementations supporting the PPP multilink protocol. This is done by defining the Bandwidth Allocation Protocol (BAP), as well as its associated control protocol, the Bandwidth Allocation Control Protocol (BACP). BAP can be used to manage the number of links in a multilink bundle.

baud rate: The rate of the signaling speed of a transmission medium.

bit: A binary digit; the smallest unit of data in the binary counting system. A bit has a value of either 0 or 1.

bits per second (bps): A measure of the actual data transmission rate. The bps rate may be equal to or greater than the baud rate depending on the modulation technique used to encode bits into each baud interval. The correct term to use when describing modem data transfer speeds.

bps: See *bits per second*.

branch: A length of cable in a star network that goes from the center of the star to a wall jack.

broadcast: A network transaction that sends data to all hosts connected to the network.

Burstiness: Data that uses bandwidth only sporadically; that is, information that does not use the total bandwidth of a circuit 100 percent of the time. During pauses, channels are idle; and no traffic flows across them in either direction. Interactive and LAN-to-LAN data is bursty in nature, because it is sent intermittently, and in between data transmission the channel experiences idle time waiting for the DTEs to respond to the transmitted data user’s input of waiting for the user to send more data.

byte: A group of bits, normally eight, which represent one data character.

CallerID: See *CND.*

CCITT (Comite Consultatif International Telegraphique et Telephonique): International Consultative Committee for Telegraphy and Telephony, a standards organization that devises and proposes recommendations for international communications. See also *ANSI (American National Standards Institute)*.

CHAP (challenge handshake protocol): A method for ensuring secure network access and communications.

Class A, B, and C networks: The values assigned to the first few bits in an IP network address determine which class designation the network has. In decimal notation, Class A network addresses range from 1.X.X.X to 126.X.X.X, Class B network addresses range from 128.1.X.X to 191.254.X.X, and Class C addresses range from 192.0.1.X to 223.255.254.X. For more information on IP network address classes, see Appendix C, "Understanding IP Addressing."

client: An intelligent workstation that makes requests to other computers known as servers. PC computers on a LAN can be clients.

clustering: A feature that clusters remapped network numbers into a range of sequential network numbers.

CNA (Calling Number Authentication): A security feature that will reject an incoming call if it does not match the Calling Number field in one of the Netopia ISDN Router's Connection Profiles.

CND (Calling Number Delivery): Also known as caller ID, a feature that allows the Called Customer Premises Equipment (CPE) to receive a calling party's directory number during the call establishment phase.

community strings: Sequences of characters that serve much like passwords for devices using SNMP. Different community strings may be used to allow an SNMP user to gather device information or change device configurations.

CRC (Cyclic Redundancy Check): A computational means to ensure the integrity of a block of data. The mathematical function is computed, before the data is transmitted at the originating device. Its numerical value is computed based on the content of the data. This value is compared with a recomputed value of the function at the destination device.

DCE (Data Communications Equipment): Term defined by standards committees, that applies to communications equipment, typically modems or printers, as distinct from other devices that attach to the network, typically personal computers or data terminals (DTE). The distinction generally refers to which pins in an RS-232-C connection transmit or receive data. Also see *DTE*.

DDP (Datagram Delivery Protocol): Defines socket-to-socket delivery of datagrams over an AppleTalk internet.

DTE (Data Terminal Equipment): Term defined by standards committees, that applies to communications equipment, typically personal computers or data terminals, as distinct from other devices that attach to the network, typically modems or printers (DCE). The distinction generally refers to which pins in an RS-232-C connection transmit or receive data. Pins 2 and 3 are reversed. Also see *DCE*.

default zone: When a Phase II EtherTalk network includes more than one zone, all routers on that network must be configured to assign one of these zones as a default zone. The default zone is temporarily assigned to any Phase II EtherTalk node that hasn't chosen a zone. The user may choose another zone by opening the Network Control Panel, selecting the correct physical connection, and then choosing a zone in the scrolling field displayed.

DHCP (Dynamic Host Configuration Protocol): A service that lets clients on a LAN request configuration information, such as IP host addresses, from a server.

DNS (Domain Name Service): A TCP/IP protocol for discovering and maintaining network resource information distributed among different servers.

download: The process of transferring a file from a server to a client.

EIA (Electronic Industry Association): A North American standards association.

Ethernet: A networking protocol that defines a type of LAN characterized by a 10 Mbps (megabits per second) data rate. Ethernet is used in many mainframe, PC, and UNIX networks, as well as for EtherTalk.

Ethernet address: Sometimes referred to as a hardware address. A 48-bits long number assigned to every Ethernet hardware device. Ethernet addresses are usually expressed as 12-character hexadecimal numbers, where each hexadecimal character (0 through F) represents four binary bits. Do not confuse the Ethernet address of a device with its network address.

EtherTalk: Apple's data-link software that allows an AppleTalk network to be connected by Ethernet cables. EtherTalk is a protocol within the AppleTalk protocol set. Two versions of EtherTalk are in common use, designated as Phase I and Phase II EtherTalk.

extended network: A network using AppleTalk Phase II protocols; EtherTalk 2.0 and TokenTalk are extended networks. LocalTalk networks are compatible with Phase II but are not extended because a single LocalTalk network cannot have multiple network numbers or multiple zone names.

firmware: System software stored in a device's memory that controls the device. The Netopia ISDN Router's firmware can be updated.

gateway: A device that connects two or more networks that use different protocols. Gateways provide address translation services, but do not translate data. Gateways must be used in conjunction with special software packages that allow computers to use networking protocols not originally designed for them.

hard seeding: A router setting. In hard seeding, if a router that has just been reset detects a network number or zone name conflict between its configured information and the information provided by another router, it disables the router port for which there is a conflict. See also *non-seeding, seeding*, *seed router,* and *soft seeding*.

HDLC (High Level Data Link Control): A generic link-level communications protocol developed by the International Organization for Standardization (ISO). HDLC manages synchronous, code-transparent, serial information transfer over a link connection. See also *SDLC (Synchronous Data Link Control).*

header: In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

hop: A single traverse from one node to another on a LAN.

hop count: The number of nodes (routers or other devices) a packet has gone through. If there are six routers between source and destination nodes, the hop count for the packet will be six when it arrives at its destination node. The maximum allowable hop count is usually 15.

hop count reduction: A feature of AURP supported by the Netopia ISDN Router. Tunnels and point-to-point links over WANs can often exceed the maximum allowable hop count of 15 routers. Network administrators can use the hop count reduction feature to set up tunnels and point-to-point links that exceed the 15-router limit.

host: A single, addressable device on a network. Computers, networked printers, and routers are hosts.

Host Computer: A communications device that enables users to run applications programs to perform such functions as text editing, program execution, access to data bases, etc.

internet: A set of networks connected together by routers. This is a general term, not to be confused with the large, multi-organizational collection of IP networks known as the Internet. An internet is sometimes also known as an internetwork.

internet address, IP address: Any computing device that uses the Internet Protocol (IP) must be assigned an internet or IP address. This is a 32-bit number assigned by the system administrator, usually written in the form of 4 decimal fields separated by periods, e.g., 192.9.200.1. Part of the internet address is the IP network number (IP network address), and part is the host address (IP host address). All machines on a given IP network use the same IP network number, and each machine has a unique IP host address. The system administrator sets the subnet mask to specify how much of the address is network number and how much is host address. See also *Class A, B, and C networks*.

IP (Internet Protocol): A networking protocol developed for use on computer systems that use the UNIX operating system. Often used with Ethernet cabling systems. In this manual, IP is used as an umbrella term to cover all packets and networking operations that include the use of the Internet Protocol. See also *TCP/IP*.

IP address, IP host address, IP network address: See *internet address*.

IP broadcast: See *broadcast*.

IP tunneling: See *AURP*.

IPX (Internet Package Exchange): A protocol used by Novell Netware networks.

ISDN (Integrated Services Digital Network): A method of transmitting data digitally over telephone lines.

ISP (Internet service provider): A company that provides Internet-related services. Most importantly, an ISP provides Internet access services and products to other companies and consumers.

ITU (International Telecommunication Union): United Nations specialized agency for telecommunications. Successor to CCITT.

K56flex: A modem data transmission technology standard created by Lucent Technologies and Rockwell International. Its purpose is to take advantage of the largely digital portions of the telephone system in order to exceed the theoretical speed limitations of data transmission over analog telephone lines. A competing technology called "x2," created by U.S. Robotics/3Com, performs a similar function. In February, 1998, the interested parties agreed on a unified standard called V.90, also known as V.PCM, which merges the K56flex standard with the competing x2 standard. In September, 1998, the International Telecommunications Union is expected to ratify the unified standard, thereby allowing interoperability of modems and ISPs' central site equipment, with appropriate firmware upgrades.

LAN (Local Area Network): A privately owned network that offers high-speed communications channels to connect information processing equipment in a limited geographic area.

LocalTalk: The cabling specification for AppleTalk running at a speed of 230.4 kbps (kilobits per second).

MacIP: A protocol in which IP packets are encapsulated within AppleTalk headers, for transmission over AppleTalk networks. MacIP requires the presence of at least one AppleTalk–IP gateway. MacIP is usually used to allow an AppleTalk computer to communicate with an IP computer.

MacIP client: A Macintosh computer that is using the MacIP protocol to communicate with an IP computer.

MIB (Management Information Base): A standardized structure for SNMP management information.

modem: A device used to convert digital signals from a computer into analog signals that can be transmitted across standard analog (not ISDN) telephone lines. Modem is a contraction of modulator-demodulator.

NAT (Network Address Translation): A feature that allows communication between the LAN connected to the Netopia ISDN Router and the Internet using a single IP address, instead of having a separate IP address for each computer on the network.

NetBIOS: A network communications protocol used on PC LANs.

network: A group of computer systems and other computer devices that communicate with one another.

network administrator: A person who coordinates the design, installation, and management of a network. A network administrator is also responsible for troubleshooting and for adding new users to the network.

network log: A record of the names of devices, location of wire pairs, wall-jack numbers, and other information about the network.

network number: A unique number for each network in an internet. AppleTalk network numbers are assigned by seed routers, to which the network is directly connected. An isolated AppleTalk network does not need a network number.

network number remapping: Resolves network number conflicts when two or more AppleTalk networks that may have duplicate network numbers are connected together. The Netopia ISDN Router lets you set up a range of network numbers into which remote AppleTalk network numbers are remapped.

network range: A unique set of contiguous numbers associated with an extended network; each number in a network range can be associated with up to 253 node addresses.

node: See *host*.

non-seeding: A router setting that causes it to request network number and zone information from any other routers on the network connected to the non-seeding port. If it receives this information, it begins to route packets through that port. See also *hard seeding, seeding*, *seed router,* and *soft seeding*.

packet: A group of fixed-length binary digits, including the data and call control signals, that are transmitted through an X.25 packet-switching network as a composite whole. The data, call control signals, and possible error control information are arranged in a predetermined format. Packets do not always travel the same pathway but are arranged in proper sequence at the destination side before forwarding the complete message to an addressee.

Packet-Switching Network: A telecommunications network based on packet-switching technology, wherein a transmission channel is occupied only for the duration of the transmission of the packet.

PAP (PPP authentication protocol): A method for ensuring secure network access.

Parameter: A numerical code that controls an aspect of terminal and/or network operation. Parameters control such aspects as page size, data transmission speed, and timing options.

port: A location for passing data in and out of a device, and, in some cases, for attaching other devices or cables.

port number: A number that identifies a TCP/IP-based service. Telnet, for example, is identified with TCP port 23.

PPP (Point to Point Protocol): A protocol for framing IP packets and transmitting them over a serial line.

protocol: A set of rules for communication, sometimes made up of several smaller sets of rules also called protocols. AppleTalk is a protocol that includes the LocalTalk, EtherTalk, and TokenTalk protocols.

remapping: See *network number remapping*.

RFC (Request for Comment): A series of documents used to exchange information and standards about the Internet.

RIP (Routing Information Protocol): A protocol used for the transmission of IP routing information.

RJ-11: A telephone-industry standard connector type, usually containing four pins.

RJ-45: A telephone-industry standard connector type usually containing eight pins.

router: A device that supports network communications. A router can connect identical network types, such as LocalTalk-to-LocalTalk, or dissimilar network types, such as LocalTalk-to-Ethernet. However—unless a gateway is available—a common protocol, such as TCP/IP, must be used over both networks. Routers may be equipped to provide WAN line support to the LAN devices they serve. They may also provide various management and monitoring functions as well as a variety of configuration capabilities.

router port: A physical or logical connection between a router and a network. Where a network only allows the use of one protocol, each physical connection corresponds to one logical router port. An example is the Netopia ISDN Router's LocalTalk port. Where a network allows the use of several protocols, each physical connection may correspond to several logical router ports—one for each protocol used. Each router port has its own network address.

routing table: A list of networks maintained by each router on an internet. Information in the routing table helps the router determine the next router to forward packets to.

seeding: A method for ensuring that two or more routers agree about which physical networks correspond to which network numbers and zone names. There are three options: non-seeding, soft seeding, and hard seeding. Seeding can often be set separately for each router port. See also *hard seeding*, *non-seeding, seed router,* and *soft seeding*.

seed router: A router that provides network number and zone information to any router that starts up on the same network. See also *hard seeding*, *non-seeding, seeding,* and *soft seeding*.

serial port: A connector on the back of the workstation through which data flows to and from a serial device.

server: A device or system that has been specifically configured to provide a service, usually to a group of clients.

SNMP (Simple Network Management Protocol): A protocol used for communication between management consoles and network devices. The Netopia ISDN Router can be managed through SNMP.

soft seeding: A router setting. In soft seeding, if a router that has just been reset detects a network number or zone name conflict between its configured information for a particular port and the information provided by another router connected to that port, it updates its configuration using the information provided by the other router. See also *hard seeding*, *non-seeding, seeding,* and *seed router*.

subnet: A network address created by using a subnet mask to specify that a number of bits in an internet address will be used as a subnet number rather than a host address.

subnet mask: A 32-bit number to specify which part of an internet address is the network number, and which part is the host address. When written in binary notation, each bit written as 1 corresponds to 1 bit of network address information. One subnet mask applies to all IP devices on an individual IP network.

SDLC (Synchronous Data Link Control): A link-level communications protocol used in an International Business Machines (IBM) Systems Network Architecture (SNA) network that manages synchronous, code-transparent, serial information transfer over a link connection. SDLC is a subset of the more generic HDLC (High-Level Data Link Control) protocol developed by the International Organization for Standardization (ISO).

TCP/IP (Transmission Control Protocol/Internet Protocol): An open network standard that defines how devices from different manufacturers communicate with each other over one or more interconnected networks. TCP/IP protocols are the foundation of the Internet, a worldwide network of networks connecting businesses, governments, researchers, and educators.

telephone wall cable: 2-pair, 4-pair, or 8-pair, 22- or 24-gauge solid copper wire cable. Telephone wall cable is sometimes called telephone station cable or twisted-pair cable.

TFTP (Trivial File Transfer Protocol/Internet Protocol): A protocol used to transfer files between IP nodes. TFTP is often used to transfer firmware and configuration information from a UNIX computer acting as a TFTP server to an IP networking device, such as the Netopia ISDN Router.

thicknet: Industry jargon for 10Base-5 coaxial cable, the original Ethernet cabling.

thinnet: Industry jargon for 10Base-2 coaxial cable, which is thinner (smaller in diameter) than the original Ethernet cabling.

UDP (User Datagram Protocol): A TCP/IP protocol describing how packets reach applications in destination nodes.

V.90: A modem data transmission standard, also known as V.PCM, which merges the K56flex standard with the competing x2 standard. In September, 1998, the International Telecommunications Union is expected to ratify the unified standard, thereby allowing interoperability of modems and ISPs' central site equipment, with appropriate firmware upgrades.

wall jack: A small hardware component used to tap into telephone wall cable. An RJ-11 wall jack usually has four pins; an RJ-45 wall jack usually has eight pins.

WAN (wide area network): A network that consists of nodes connected by long-distance transmission media, such as telephone lines. WANs can span a state, a country, or even the world.

WAN IP: In addition to being a router, the Netopia ISDN Router is also an IP address server. There are four protocols it can use to distribute IP addresses over the WAN which include: DHCP, BOOTP, IPCP and MacIP. WAN IP is a feature for both the Small Office and Corporate Netopia ISDN Router models.

wiring closet: A central location where a building's telephone and network wiring is connected. Multi-story buildings often have a main wiring closet in the basement and satellite wiring closets on each floor.

zone: An arbitrary subset of nodes within an AppleTalk internet. Creating multiple zones makes it easier for users to locate network services. The network administrator defines zones when he or she configures routers. Isolated networks have no zones. LocalTalk and EtherTalk Phase I networks may have no more than one zone each. EtherTalk Phase II and TokenTalk networks may have more than one zone each. Several networks of any AppleTalk type may share a zone name.

Index

Limited Warranty and Limitation of Remedies

Netopia warrants to you, the end user, that the Netopia R2020 Dual Analog Router (the "Product") will be free from defects in materials and workmanship under normal use for a period of one (1) year from date of purchase. Netopia's entire liability and your sole remedy under this warranty during the warranty period is that Netopia shall, at its option, either repair the Product or refund the original purchase price of the Product.

In order to make a claim under this warranty you must comply with the following procedure:

1. Contact Netopia Customer Service within the warranty period to obtain a Return Materials Authorization ("RMA") number.
2. Return the defective Product and proof of purchase, shipping prepaid, to Netopia with the RMA number prominently displayed on the outside of the package.

If you are located outside of the United States or Canada, please contact your dealer in order to arrange for warranty service.

THE ABOVE WARRANTIES ARE MADE BY NETOPIA ALONE, AND THEY ARE THE ONLY WARRANTIES MADE BY ANYONE REGARDING THE ENCLOSED PRODUCT. NETOPIA AND ITS LICENSOR(S) MAKE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE ENCLOSED PRODUCT. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED ABOVE, NETOPIA AND ITS LICENSOR(S) DO NOT WARRANT, GUARANTEE OR MAKE ANY REPRESENTATION REGARDING THE USE OR THE RESULTS OF THE USE OF THE PRODUCT IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS, OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCT IS ASSUMED BY YOU. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES OR JURISDICTIONS, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT CASE, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY OF THE PRODUCT. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM JURISDICTION TO JURISDICTION.

REGARDLESS OF WHETHER OR NOT ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL NETOPIA, ITS LICENSOR(S) AND THE DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS OF ANY OF THEM BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT THE USE OR INABILITY TO USE THE PRODUCT EVEN IF NETOPIA OR ITS LICENSOR(S) HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. NETOPIA AND ITS LICENSOR(S) LIABILITY TO YOU FOR ACTUAL DAMAGES FROM ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION (WHETHER IN CONTRACT, TORT [INCLUDING NEGLIGENCE], PRODUCT LIABILITY OR OTHERWISE), WILL BE LIMITED TO $50. v.697